IMAGE AND VIDEO SECURITY USING FRACTIONAL TRANSFORM AND MULTIMODAL BIOMETRIC KEYS

A Dissertation Submitted in Partial Fulfillment of the Requirement for the Award of the Degree of

MASTER OF ENGINEERING

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted By

JOBANPREET KAUR

REG. NO. 801561010

Under Supervision of

Dr. Neeru Jindal

Assistant Professor, ECED

Thapar University, Patiala

(Supervisor)

Dr. Sanjay Sharma

Professor, ECED

Thapar University, Patiala

(Co-Supervisor)

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY, PATIALA, PUNJAB

JULY, 2017

DECLARATION

I, Jobanpreet Kaur hereby declare that the work presented in this thesis entitled **"Image and video security using fractional transform and multimodal biometric keys"** in fulfillment of the requirement for the award of degree of Master of Engineering submitted at Electronics and Communication Engineering, Thapar University, Patiala is an authentic record of work carried out under supervision of Dr. Neeru Jindal (Assistant Professor, Thapar University) and Dr. Sanjay Sharma (Professor, Thapar University). The matter presented in this has not been submitted either in part or full to any other university or institute for the award of any other degree.

Jobanpreet Kaur

Date: 22-08-2017

Jobanpreet Kaur

801561010

It is certified that the above statement made by the candidate is correct to the best of my knowledge and belief.

Dr. Neeru Jindal

Assistant Professor, ECED

Thapar University, Patiala

(Supervisor)

Dr. Sanjay Sharma

Professor, ECED

Thapar University, Patiala

(Co-Supervisor)

ACKNOWLEDGEMENT

First and foremost, I would like to thank GOD for showering His blessing upon me during the complete work duration and providing me courage and ability to work against all odds.

Besides, I would like to express my sincere gratitude to my research advisor Dr. Neeru Jindal (Assistant Professor) and Dr. Sanjay Sharma (Professor), ECED, Thapar University, Patiala for their support, patience, motivation, enthusiasm and guidance during my course work. I have been inspired by their diligence, attention to describe and their vigorous application to any problem. I value their worry and support at all times. They have always emphasis on self-motivation during rough or bad periods and appreciated in good days. The words are not enough to thank them.

I am also thankful to Thapar University for the facilities and healthy environment for study. I also convey my sincere thanks to the Head of the Department, Dr. Alpana Aggarwal for providing me adequate environment in carrying the work.

I am highly obliged and wish to owe my sincere gratitude to Dr. Amit Mishra,, Program Coordinator ME, ECE and Dr. Hem Dutt Joshi, P.G. Coordinator, Electronics and Communication Engineering Department, Thapar University, Patiala for providing me facilities, learning atmosphere and infrastructure in ECED.

Finally, I must express my very deep gratitude to my parents and friends for providing reliable support and continuous encouragement throughout my years of revision and through the process of researching and writing this thesis. This completion would not have been possible without them.

(Jobanpreet Kaur)

ABSTRACT

In today's world, as the use of internet has facilitates humans in several areas such as transferring information, instant messaging, video conferencing etc. It also adds on need of security techniques to protect these multimedia contents in communication from intruders. To fulfil this security need, this thesis work has been proposed to secure images and videos transferred in the open channel. For the security of multimedia contents (i.e. images and videos) several techniques have been invented, but encryption is used in proposed work to create chaos in the transmitted information. Due to presence of uncertainty in the ciphered information, it became difficult for the hacker to differentiate between random noise and ciphered data. Further, encryption can be performed with several techniques AES (Advanced Encryption Standard), chaotic mapping, Arnold transforms, matrix transformation and fractional transforms etc. The proposed work is about **"Image and video security using fractional transform and multimodal biometric keys"**. The fractional transforms are preferred for the encryption because it provides extra degree of freedom, due to presence of non-integer fractional order. To add on more security features to the algorithm combination of fractional transform and scrambling has been used in proposed algorithm. Due to unique and untraceable features of biometrics, the threat of tracing key has been conquered.

After implementing encryption algorithm for the security of images and videos, performance parameters like PSNR (peak signal to noise ratio), MSE (mean square error), SSIM (structural similarity index measure), correlation between adjacent pixels and histogram analysis have been computed to improve capability of the proposed algorithm. The proposed algorithm provides infinite PSNR and zero MSE that shows better performance of proposed algorithm than existing ones. The various attacks like differential attacks, brute force attacks, known plaintext attacks etc. have been applied on the encrypted information to check the attacks resistance power of proposed algorithm. Hence, the use of biometric keys provides attack resistance power to the algorithm.

Thus, the comparison between the parameters of proposed and existing algorithms verifies the improvement in proposed algorithm. In future scope, even more secured and complex transform can be invented to improve the efficiency of proposed algorithm.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
ATM	Automated Teller Machine
BFA	Brute Force Attack
CATV	Community Access Television
CCA	Chose Ciphertext Attack
COA	Cipher Only Attack
CR	Compression Ratio
CSA	Common Scrambling Algorithm
DC	Discrete Cosine
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DFrCT	Discrete Fractional Cosine Transform
DFrFT	Discrete Fractional Fourier Transform
DP-FrFT	Dual parameter based Fractional Fourier Transform
DP-FrWT	Dual parameter based Fractional Wavelet Transform
DVB	Digital Video Broadcasting
ETSI	European Telecommunications Standards Institute
FMO	Flexible Macroblocks Ordering
FrCT	Fractional Cosine Transform
FrFT	Fractional Fourier Transform
FrHT	Fractional Hartley Transform
FrMT	Fractional Mellin Transform
FrWT	Fractional Wavelet Transform
FT	Fourier Transform
GME	Gradient Magnitude Error
GMSD	Gradient Magnitude Similarity Deviation
GMSM	Gradient Magnitude Similarity Mean
GPE	Gradient Phase Error
GSM	Gradient Magnitude Similarity

HD	Hamming Distance
IBM	International Business Machines
JQI	JPEG quality Index
KPA	Known Plaintext Attack
LMSE	Laplacian Mean Square Error
LQM	Local Quality Measure
MAMS	Mean Angle Magnitude Similarity
MAS	Mean Angle Similarity
MIM	Man In Middle Attack
MPEG	Motion Picture Experts Group
MP-FrFAT	Multiple Parameter Fractional Fourier Arnold Transform
MSE	Mean Square Error
NPCR	Number of Pixels Change Rate
PSNR	Peak Signal Noise Ratio
ROI	Region of Interest
RSA	Rivest, Adi Shamir
SD	Spectral Distortion
SSIM	Structural Similarity Index Measure
STFT	Short Time Fourier Transform
STFrFT	Short time Fractional Fourier Transform
TCD	Total Corner Difference
TED	Total Edge Difference
TV	Television
UACI	Unified Average Changing Intensity
VEA	Video Encryption Algorithm
XOR	Exclusive OR

CHAPTER 1

INTRODUCTION

1.1 PROLOGUE

An image is a two dimensional signal, which is represented in the form of matrix consisting elements known as pixels. An image is worth representing thousands of words and video is defined as sequence of frames or still images.

In this modern era, the transfer of multimedia information is increasing very rapidly, due to frequent use of internet. The use of images and videos is prevailing very rapidly through various applications such as biomedical images, video telephony, internet video, video conferencing, military communication etc. are being used now days. So, the security of information is very important aspect of communication. The transferring medium is freely available for exchanging information between sender and receiver, but intruders are also welcomed in it. They can easily hack the contents from the channel and modify it before reaches at the reception end or misuse it. In this way, any person can hack the confidential information or can harm the reputation of person or organization. So, there is need to protect this information from getting stolen or modified while transferring through the medium. The protection can be given by using protected environment or by encoding information. The security of environment is difficult task; solution is to convert information into randomized form to protect it from invaders. Although several techniques are available like DES (Digital Encryption Standard), AES (Advanced Encryption Standard), RSA (Rivest Shamir Adleman) [1] for various applications and the fractional transforms has been used in this thesis.

1.2 FRACTIONAL TRANSFORMS

The fractional transforms were introduced to enhance the performance parameters for various applications. Before the invention of fractional transforms, the Fourier Transform (FT) was initially invented by Jean-Baptiste-Joseph Fourier [2]. FT has been used for several applications in various fields such as image processing, signal analysis, physics, optics, statistics and antenna etc. The generalization of FT gives birth to fractional Fourier transform (FrFT) and used as basic tool for various fractional transform in image encryption.. The FrFT was firstly invented in 1929 [3]. The idea of FrFT was discussed by several authors in successive times, but with different names. FT was providing good results, but it cannot be implemented on non-stationary signals, so FrFT comes into play. Then, in 1980 V. Namias

invented that all other transforms can also be fractionalized [4]. For the study of finite signals FT was converted into Discrete Fourier Transform (DFT) and FrFT is converted into discrete fractional Fourier transform (DFrFT). The DFrFT is defined as the linear transformation in which definition of the transform is n^{th} power and n is not necessary to be integer, thus it can transform image into any intermediate domain. The several Fractional transforms that are used for the image encryption are fractional cosine transform (FrCT) [5], fractional wavelet transform (FrWT) [6], dual parameter based fractional Fourier transform (DP-FrFT) [7], fractional Hartley transform (FrHT) [8], fractional Mellin transform (FrMT) [9] etc. From these fractional transforms, fractional Fourier transform and fractional wavelet transform are accounted in this thesis for the security of information.

The fractional transforms are mostly used for several purposes such as encryption, compression, noise reduction, filtering etc. The encryption techniques are further separated into two types, full encryption and partial encryption. The choice is based upon the requirement of application.

1.3 IMAGE AND VIDEOS ENCRYPTION METHODS FOR SECURITY

There are various techniques like Steganography, watermarking, cryptography available for the security of information from the invaders. Among these techniques, Steganography is used to embed the text into another image for the protection of text [7]. In watermarking, the original image is applied as watermarked image on cover image [11]. In cryptography, the whole image is transformed in such a form that is difficult for the interloper to comprehend it, so used for the protection of images [12] and videos. Every security technique has its own significance and applications. But, encryption is one of the best methods used in cryptography for security of images and videos. This method is performed to create confusion and diffusion in the images and videos (or frames of videos). Due to presence of chaos in the ciphered information, hacker will consider information as random noise. The appearance of encrypted form will protect information from getting stolen. Further, encryption can be performed with different algorithms to hide actual data from hackers. The several techniques available for encryption algorithm are chaotic mapping [13], matrix transformation [14], scrambling [15], and compression and encryption using wavelet transform [16] etc. To increase the security level of encryption, new and better algorithms are always welcomed. The various methods that can be applied for encryption of multimedia content (i.e. images and videos) are given as follows:

1.3.1 Full Encryption

In full encryption, chaos is created in the whole image and then that image is transferred by sender and transmitted through the channel. For highly confidential information, full image is distorted to this extent that it is difficult for the unauthorized person to figure out it, without the information of actual algorithm that is performed on the images or videos. Several techniques that are available for encryption process are permutation and XOR operations [17], block shuffling and chaotic mapping [18], and fractional cosine transform [8] etc. This type of encryption consumes time, but provides secure communication without any chance of leakage. All these techniques are used for the encryption process in order to protect them from the external attacks.

1.3.2 Partial Encryption

Partial encryption is one of the types of encryption. In this particular region of image or frame of video is encrypted to keep that area confidential. So, for this process region of interest (ROI) is selected and then only that region is processed further for selective encryption using various techniques such as wavelet transform [16], block shuffling and Arnold transform [19], and logistic chaotic mapping [20] etc. In some cases the whole frame is partially encrypted and choice about the selective partial or whole partial encryption is totally based upon the type of information that needs security.

1.3.3 Scrambling

Although, several techniques are available for the encryption, but implementation of that techniques is very complex. In the method of encrypting images and videos using scrambling process, the position of pixels in the image is shuffled in order to create anarchy in the original information. Scrambling is simple technique that is applied on the images for its protection [15]. The ultimate goal is to disorder the imaged for its security, so that can be protected from hackers. The encrypted image looks like any noise present in the network, except from sender and receiver no one has any idea about it. But for highly confidential data, this technique is very simple and can be used with some other technique for better security,

Although, these methods are available for encrypting images and videos, but the essential part of every technique is the key. The security of any method is dependent on type of key chosen for encryption procedures, so choice of key is very important aspect. The key can be generated mathematical algorithms or with the features of biometrics.

1.4 ENCRYPTION KEYS

Encryption algorithms are used for the secrecy of the multimedia information from the invaders. The key used for the encryption decides the quality of encryption technique. The types of keys used for the encryption are asymmetric keys and symmetric keys [10] as shown in Figure 1.1. The choice of key used for the encryption is reliant upon the type of application, for which security is required. Now a day's the use of biometric keys has been increased due to uniqueness in features of biometrics. These keys are demonstrated as follows:

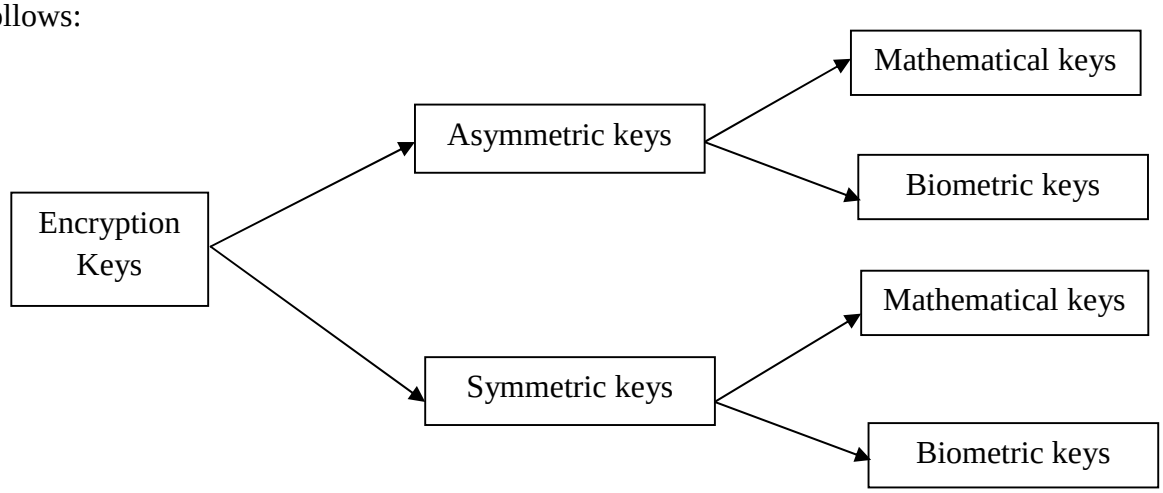


Figure 1.1 Types of encryption keys

1.4.1 Asymmetric keys

An asymmetric key encryption is one of the methods used for the encryption process. In this technique, two keys are required for the encryption and decryption of the images and videos. Here, public key is applied in encryption process and private key is applied by receiver for the decryption of encrypted multimedia information. In the color image encryption [22] is performed used asymmetric key encryption is performed using Hartley transform, random phase masks and transform angle of gyrator transform are used. In this way two different keys are used at sender and receiver side of information. In proposed thesis, video encryption has been performed with asymmetric key generated by using iris and fingerprint.

1.4.2 Symmetric keys

The symmetric key encryption is that technique in which same key is used at the sender and reception side. The symmetric keys can be generated using mathematical algorithms or using biometric. Although, use of asymmetric keys will provide better safety for multimedia data, but symmetric keys like biometric keys are also one of the best keys to provide secured

environment to multimedia contents. The image encryption is performed using integer wavelet transform in combination with symmetric key generated using logistic chaotic mapping [23].

1.4.3 Biometric keys

Biometric keys are considered as more secure as compared to mathematical keys, because of their unique features and untraceable behavior. These keys can be used in combination with mathematical keys for the better security of multimedia content [7]. In modern era of internet, preference is given to several biometrics keys to keep the privacy of information.

All above methods are used for the encryption algorithms for multimedia encryption procedures, but still there is requirement of more powerful technique for the better results. So, in order to keep this need in mind this thesis proposed fractional transforms for the encryption processes in combination with biometric keys in order to protect information from various hackers has been introduced in proposed work.

1.5 THESIS ORGANIZATION

This thesis comprises chapters as follows:

Chapter 1 consists brief introduction about the need of security, encryption methods, encryption keys and discusses about fractional transforms used for the encryption purposes.

Chapter 2 discusses about the development made in area of fractional transforms for compression and encryption of images and videos to protect them from intruders, also explains scrambling and biometric keys for the security of information.

Chapter 3 consists mathematical study of fractional transform and scrambling used in the proposed work.

Chapter 4 includes the algorithm used for the image encryption using dual parameter based fractional wavelet transform and scrambling in combination with symmetric multimodal biometric keys. It also consists of simulation results on some test images with several performance parameters.

Chapter 5 briefs about the technique used for the ROI based encryption of videos and its simulation results using some test videos. It also discussed the comparison of proposed technique with existing techniques.

Chapter 6 sums up the improvement in the proposed technique in comparison with existing algorithms and ends with the future scope for proposed work.

CHAPTER 2

LITERATURE SURVEY

This chapter includes the precise literature of encryption techniques, which is considered as most effective method to attain data security. In this thesis, fractional transforms and scrambling in combination with duo biometric keys are used for providing security to the multimedia.

2.1 INTRODUCTION

Earlier the cryptography was performed only on text message, in order to convert it into non-understandable form to protect it from eavesdroppers. Cryptography was initially used in old kingdom of Egypt in 1900 for hiding formal writing of Egyptians. Then, in the time of Greeks, another technique was used by military for keeping confidentiality of information using Steganography [24]. Most of the time the information is hidden in the form of puzzles and that can be easily solved by the intruder and data is modified or stolen before it reaches at the reception end. Then, in 9^{th} century frequency analysis has been discovered by Arabs [25]. In this way frequency analysis has become very powerful technique to provide security, because knowledge of key is required to break the security of deformed data. So, it was realized in 19^{th} century that security of key is an important issue. After that in 20^{th} century several encryption and decryption devices were used by Germany's military and government for the protection of secret information till World War II [26], but they used hardware devices for protection of information, which is complicated method and cannot be used anymore due to difficulty in management of these procedures. Then, in order to provide handy methods digital computers were invented to abolish the problems of handling complex algorithms. The extensive use of cryptography had been developed in 1970s after IBM personnel designed DES (Data Encryption Standard) algorithm [24] and some key arrangement techniques were also invented in 1976 [27]. After that many algorithms (such as RSA algorithm) were designed by several designers according to requirement of various applications. Then continuous improvement was being made by making use of mathematics in encryption algorithms like information theory, statistics, number theory computational complexity and finite mathematics. To protect data from brute force attacks key length is increased. So, modern cryptography has developed various other mathematical techniques for better results like transforms, scrambling, DES, etc. In this thesis work is done using fractional transforms

and scrambling in combination with duo biometric keys to secure images and videos transmission from intruders.

2.2 FRACTIONAL TRANSFORMS

The concept of fractional was invented in 17th century by Bernoulli, by arising question about non-integer order of derivative [7]. It leads to the beginning of fractional differential equations. The requirement of application area of FT had introduced fraction in 1929 that lead to FrFT to add extra degree of freedom to FT. Thus, the concept of fractional calculus was developed in optics and signal processing by the mathematician. Then, further the work on the FrFT was done in 1930 by H. Weyl to introduce the concept of FrFT to the world. Afterwards, in 1937 E. U. Condon, who is followed by H. Kober in 1937, in 1956 A. P. Guinanad, in 1959 A. L. Patterson, in 1961 V. Bargmann, in 1973 by De Brujin and in 1974 finally by R. S. Khare [28]. In this way finally use of fractional transforms were used in applications to improve the results of various techniques [8-12].

2.2.1 Fractional Fourier Transform (FrFT)

The FrFT was initially introduced by Namias in 1980, unknown by the fact of its invention in 1929, as advanced version of FT. The definition and properties of FrFT were introduced by Almeida. FrFT is defined as the time frequency conversion which disclosed the change in properties of signals during its transformation from time to frequency domain with the variation in transform order between 0 and 1. Kutay *et al.*, the work done so far was not applicable to digital computations [29].

The incompatibility problem of DFrFT developed so far doesn't offer the same results as given by continuous FrFT. The DFrFT was formed by combining actual signal, circular flipped signal, DFT of signal and circular flipped DFT of signal as documented [29]. Then, an accurate and improved algorithm to get better as fractional Fourier transform was proposed by Ozaktas in 1996. The computation of FrFT didn't require oversampling by factor defined by transform order instead it requires factor of two. After that due to increase in digitalization, the DFrFT had been improved. In DFrFT, the signal recovered included some approximation errors.

Dickinson followed by Santhanam *et al.* introduced FrFT with entirely different manner. Then, Cariolario [29] developed FrFT for all types of signals *i.e.* discrete and continuous, single and multidimensional etc. A new approach using computers has been put forward in last decade known as discrete FrFT which facilitates the physical and mathematical analysis

of signals. It also introduced an extra degree by developing discrete fractional transforms. The more improvement in DFrFT was involved in 1996. The DFrFT provides same frequency and time characteristics of signals.

Then, Pie *et al.* in 2000 classified many definition of FrFT as per methodology used for the computations. The easiest way is to sample the continuous FrFT to get the Discrete FrFT and do computations, but it didn't provide the much better results as it loses various properties. Then, superior sampling type introduced, but it was suitable for some signals only. Although many definition of the FrFT exists but none of them satisfies all properties of fractional Fourier transform and neither of them provides perfect mathematical definition of discrete FrFT [26].

The various applications of FrFT are images and signal recovery [29], signal detector, pattern recognition, signal processing in optics, time or space variant filter etc. The use of DFrFT has been extended now a day for various applications such as watermarking, signal restoration, tomography, multiplexing, filtering, encryption [10], compression etc.

2.2.2 Dual parameter based fractional wavelet transform (DP-FrWT)

Already, history of fractional Fourier transform had been discussed in previous section, although it has been used for several applications but need to have better transform never ends. The FrFT doesn't provide any idea about time localization of spectral components of FrFT [30]. To solve the difficulty in study of non stationary signals, whose spectral characteristics of FrFT changes with the time, requires transform which measures the signal variations both in FrFT and time domain. To overcome this problem, initially FrFT has been modified to short time FrFT (STFrFT) [30]. The use of STFrFT comes into play to segment the signal into time domain window and applying FrFT on every segment. In this way STFrFT was able to provide solution of above stated crisis in FrFT. The other problem in use of STFrFT is fixed length of window that too requires to be fixed before computations, that doesn't provide superior resolution to the output. If window size is small, it will offer good time resolution, but poor spectral resolution, if window size is broader then it will provide good spectral resolution, but bad time resolution. To resolve problem of spectral and time resolution, David Mendlovic *et al.* generalized the wavelet transform into fractional wavelet transform (FrWT). Then, Akhilesh Prasad *et al.* provide mathematical expression for the FrWT. transform (FrWT). Then, Akhilesh Prasad *et al.* provide mathematical expression for the FrWT. Now recently Shi et al. introduced new explanation to FrWT associated with FrFT.

The use of fractional wavelet transform provides better results for various applications like detection of chirp, selective encryption, differential equations, denoising. These are some of the applications, where fractional wavelet transform gives better output then existing techniques and also open areas for new applications.

It has been concluded that FrWT resolved most of the problems faced in FrFT [30]. Gaurav *et al.* [7] introduced new dual parameter fractional Fourier transform (DP-FrFT) for security of the images using encryption process in combination with single biometric key. So, in this thesis dual parameter based fractional wavelet transform in joint with scrambling algorithm has been introduced that provides good results than existing algorithms. The use of asymmetric biometric key also provided highly secure environment for the communication of images and videos through open network.

2.3 REVIEW OF IMAGE SECURITY TECHNIQUES

Images are very important part of communication. A single image contains information more than thousands of words, due to that images are used in many areas for representation of confidential information. So, the basic requirement is to protect the images from the hackers. To accomplish this need several techniques are presented, but in this thesis encryption techniques are chosen to secure images from intruders. Some techniques are discussed further based upon encryption and scrambling of images using several algorithms.

2.3.1 Encryption Techniques

Image security is increasing very alarmingly in modern world, due to very frequent use of internet for communication. In order to protect the information from the intruders several methods are available with different algorithm, but encryption creates more confusion to the images than other techniques. So, the information received after encryption is unpredictable without the information of keys. The security of several biometrics or other confidential images promotes the use of encryption techniques. Recently, to avoid the cost of transferring any medical forms from clinical labs, they are converted into electronic form and communicate through the internet towards medical centers. So, these reports need to be kept secretly from any unknown person due to that this information is encrypted before sending it towards its destination point. Although many algorithms are available for the encryption of images, but the use of fractional transform is preferred because of number of keys provided in the encryption algorithm [7].

From last decade optical communication started the use of FrFT [31] for encryption. Then, Hennelly *et al.* in 2003 developed phase retrieval technique for image encryption using FrFT [32]. After that Hennelly *et al.* gives survey of encryption techniques using FrFT in optics [33]. The parameter used to measure the quality of decrypted image than original image was mean square error (MSE).

Initially, Fourier transform is used for encryption in optics [34], the extra degrees provided by FrFT were not being used. Then, further development in optical communication systems made proper use of FrFT [35]. After this development, additional keys were provided by FrFT and random phase keys are used for encryption algorithms to provide better security to the images [36].

Some other methods were also invented to improve the results of encryption techniques in optical communication. The methods developed use any number of phase keys and FrFT process to get encrypted information [37]. The other algorithm invented for encryption in combination with FrFT was convolution operation [38].

As, it is well known that fresh and better algorithm are always welcomed. So, with modification in fractional Fourier transform new methods were invented. By making use of periodicity property of FrFT new technique was derived [27]. The random shifting algorithms without using phase keys encrypt the images in similar manner [32].

The multiple order FrFT was invented to encrypt the images in optics [39]. In this way more improvement is going on to get better results. Then, after some time dual parameter based FrFT was introduced to use both transform order as well as transform angle for the encryption of images in combination with biometric keys [7] to increase the security level of encryption process.

2.3.2 Scrambling Techniques

Scrambling is also one of the algorithms used to keep confidentiality of images.The new methods were developed in 2003 for digital images [40]. One of them was based on 3D Arnold transform and other is implemented using gray code transformation. Then, other scrambling algorithm is applied using Fibonacci series [41]. The pros of scrambling are (i) scattering of information in whole image (ii) protect it against data loss, common attacks and noise (iii) encryption and decryption is simple in real world. After that instead of using two steps for scrambling queue transformation provides single step scrambling in 2007 [42]. Due

to use of single step process, the reference point can be changed every time to protect it from hackers. Another methods developed for the scrambling were based on queue transformation and wavelet transformation in 2008 [42], [43] with good degree of scrambling. In 2008, the scrambling is also performed using random shuffling of the positions of pixels with provided shifted path [44].

Although several algorithms are available for the scrambling operation, the best method will be considered on its ability to resist various noise attacks such as salt & pepper, Gaussian noise, ciphertext attack etc. [37].

The use of both encryptions and scrambling techniques provide good quality of encryption, that is calculated using mean square error (MSE), peak signal to noise ratio (PSNR) etc. to show improvement in proposed technique than existing techniques. For security of images other techniques are also available, one of them is discussed in further section.

2.4 PRELIMINARIES OF VIDEO SECURITY TECHNIQUES

In the several applications of video processing like business conferencing, military communication etc., the content of videos is required to be preserved. So, for the preservation of video information security techniques are required. To meet this requirement several techniques had been invented. In this thesis, encryption and scrambling based security techniques are discussed.

2.4.1 Encryption Techniques

Cryptography (encryption and decryption) was initially used by ancient Egyptians [45]. They were very much concerned about the privacy of information. The cryptography was important technique used in Second World War by allied forces and helps them to defeat their enemies sooner [46]. Cryptography was also used by allied forces to resolve the Enigma machine used for encryption to protect their confidential military communication [47]. Here, in this thesis main focus is on the security of video based information from the unauthorized receivers.

The video is series of images [48]. The security level of video is dependent on type of applications. Due to chain of images space for storage of videos and bandwidth for transfer of videos required is large. So, in order to save the bandwidth and storage space for the videos compression is taken into account. After compression, encryption is applied on the frames of the videos. The encryption of full video frames was going smoothly with various techniques for several applications, but the computational time of algorithms was still very high. To

overcome this problem, the method of selective encryption or partial encryption of videos was suggested. Thus, the amount of power consumed for encrypting video content was also reduced. All these factors encourage the use of partial encryption algorithms.

In 1995, Jurgen introduced selective encryption technique for MPEG-1 video streams named as SECMPEG (Secure MPEG) [49]. In this algorithm, four security levels are defined in which (i) the header of the video layer was encrypted (ii) DCT coefficient of low frequency blocks of I-frames are encrypted (iii) I-frames and I-blocks of P and B frames were encrypted (iv) whole video of MPEG standard is encrypted. The security levels of (iii) and (iv) level was higher to prevent sequence from all the attacks. Then, Agi *et al.* demonstrated about the leaks in above mentioned technique, the P and B frame would be easily decrypted without the information of key applied on the algorithm [50], only 30-60 percentage of data was included in I -frame [51] of computation time is not affected much.

To resolve above stated issue, George *et al.* [52] suggested new technique to secure MPEG standard videos. In this procedure, only I-frame and header sequence of the video is encrypted. Header included all the information about the frame bit rate, height, width, buffer size and frame rate. DES encryption algorithm was used for the encryption, named Aegis mechanism. Gong *et al.* [49] in 1996 found that encryption of only I-frame is fine for some of the applications, but not for all the applications. In some videos, P and B frames also conveyed some of the scenes of video and broke the advantages of security techniques. In highly secret communications like military communication, business related conferences etc. can't take risk of using Aegis mechanism. Although, it can be used for the applications like TV broadcasting or entertainment purposes, where security of video is not bigger issue.

A new technique proposed by Lintain *et al.* called VEA (Video Encryption Algorithm) [53]. It depends upon the symmetrical key algorithm and statistical properties of videos. This encryption is performed on MPEG standard videos. In this algorithm the video is divided into chunks. Then, that chunks are further divided into odd and even lists. Initially, encryption method is applied on the even list, after that encryption result is concatenated with odd list of video chunks. In this way video is protected from KPA (known plaintext attacks). After this four new algorithms were demonstrated by Bhargava *et al.* [54]. In 1998 first algorithm was introduced in which compression ratio is saved by permuting MPEG with Huffman code list. But this method was susceptible to known plaintext attack and ciphertext only attack. To remove this limitation from the algorithm in 1999 by Bhargava *et al.* [55] where encryption is performed only on the DC coefficients with sign bits. The whole algorithm is dependent upon

the length of the key, but key should be of realistic length. So, in this algorithm key length decides the level of security for videos. In third algorithm, to make algorithm invulnerable to attacks, by making the motion vectors from P and B frames, and sign bits of DC coefficient having differential values are encrypted by applying XOR operation with cipher key. But, in third algorithm one issue related to attacks was resolved while other problem of key length remained there. In 1999, fourth algorithm invented in which symmetric key based encryption was applied on motion vector and DC coefficients of sign bits. It increases the computational speed, to improve effectiveness of algorithm. A performance of fourth algorithm is better than other existing methods.

Until now, most of the algorithms were based upon the DES, AES and VEA algorithms, then in successive years the improvement is being made to protect video from several attacks as well as to increase the computational speed of the algorithm. Several authors using different techniques were able to give good results. Some other techniques used for the selective video encryption are unitary transform [56], multiple transform [57], FMO (Flexible Macroblock ordering) and chaos [58], random permutation based [59], Zig-Zag randomized scanning [60] etc.

Although all the above methods used for selective video encryption provide good results, in order to get better results of algorithm, new methods are required. The fractional transforms are doing wonders in various applications such as video conferencing etc., but the use of fractional transform in case of video encryption is still limited.

2.4.2 Scrambling Techniques

Scrambling is defined as one of the encryption technique used to create chaos in the data to make it in unreadable form. It is also called as common scrambling algorithm (CSA). CSA was initially stated by ETSI (European Telecommunication Standards Institute) and in 1994 used for the Digital Video Broadcasting (DVB). After that CSA was followed by CSA3 in combination with AES (Advanced Encryption Standard) of 128-bits. The use of CSA was not remarkable so usually used for the protection of DVB [61]. Earlier, the use of scrambling was kept secretly to protect its confidential use [61]. Although hints were given in some patent papers, but the exact algorithm was not known. Initially, the implementation of the scrambling is done with hardware only.

In 2003 Zeng *et al.* designed technique for the security of videos with combination of scrambling and compression [62]. In this simple scrambling algorithm was used for the

protection of videos from external attacks, without affecting the efficiency of compression applied on it. It was used for flexible partial encryption and provides transparency and scalability. After that, Tang [63] introduced another technique which performed compression and encryption in one step. A very simple technique was invented to reduce computational time. Then, Wang e*t al.* [64] proposed new technique in which scrambling with DCT coefficient was used for the encryption process. The limitation of pirating videos and external attacks were prevented with the use of this process.

In this way the work on videos using scrambling is limited, because scrambling is simple technique and it can be cracked by hit and trail method. In order to enhance security of communication system, better security technique can be invented by combining scrambling with some other encryption techniques. In encryption techniques, the basic requirement is encryption key. The key decides the superiority of the encryption process, because it preserves the features of actual information.

2.5 BIOMETRIC ENCRYPTION KEYS

The security of algorithm relies upon the selection of keys used in the algorithm. So, the choice of key is really very important matter for encryption. In most of the encryption techniques, the keys used are either symmetric mathematical keys or asymmetric mathematical keys [14]. In symmetric mathematical key, same key or password is required at the receiver to extract original information from the encrypted information, but in asymmetric mathematical keys public key is used at transmitter side and private key is used at receiver side. The mathematical keys can be guessed, so other better option to keep confidentiality is making use of biometric keys, because they are unique and untraceable. So, the pattern extracted from biometric of every person is inimitable. In order to keep the biometrics safe from the intruders, spoofing attacks are also considered while using biometric keys. For generating even better algorithm, both mathematical as well as biometric keys can be used for encryption process. The generation of various biometric keys is discussed in Table 2.1. It concludes the several algorithms that are used for generation of keys from some of the biometrics for the security purposes in various applications. It also sums up some gaps as well that can be taken in consideration while generating keys from biometrics, so that for generating biometric keys strong method can be introduced, which doesn't allow the information leakage through it. Due to these reasons biometric keys are preferred than other keys. There are many biometrics available that can be used to generate key for the encryption process, but mostly used biometrics are given in Figure 2.1.

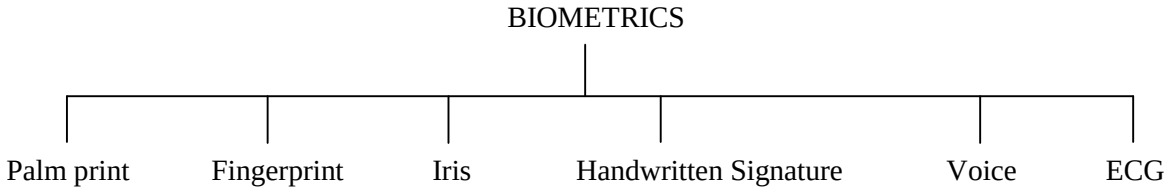


Figure 2.1 Biometrics keys used for encryption

Name of Biometric	Author Name and Year	Description	Gaps
Voice[65]	Fabian *et al.*, IEEE, 2001	The features of words utter from the mouth of person are used. Initially, features are extracted and then key is generated from them.	The voice of person can be recorded and used at the reception side to extract the information secured by using voice.
Face[66]	Wende *et al.*, IEEE, 2001	The face of person has several different features that are used to generate key after performing thresholding on them.	Regular updating is required due to change in features of face with passage of time.
Iris[67]	John, IEEE, 2004	Iris is most delicate part of eye that is not affected by the external environment. So, features of iris are extracted from the scanned eye image using circular Hough transform.	Although iris is very effective biometric, but combination of some other biometric can provide even better results.
Fingerprint [68]	Nguyen *et al.*, IEEE, 2008	Fingerprints cannot be forged, so they can be used for the generation of key from its minutiae.	Fingerprints fade away during passage of time by doing physical work, updating is required with time.
Handwritten Signature[69]	Sanaul *et al.*, IEEE, 2008	Handwritten signature is real time biometric that is used as key for the security purposes. It has 45 features that are extracted to compare the change in original and false handwritten signatures.	This key generation is specifically recommended for symmetric key encryption.
Palm Print[70]	Xiangqian *et al.*, IEEE, 2008	Extracted features of palm print are used to generate DoG (Derivative Of Gaussian) codes with Gaussian Derivative filters. With this less false rejection ratio and better security is achieved.	For better security and more secure biometric keys chaotic mapping can be used to get final key.
ECG(Electrocardiogram) Signals[71]	Ching *et al.*, IEEE, 2010	To meet the need of security, ECG is also involved. Key is generated using ECG signal in combination with logistic chaotic mapping.	In this encryption system is more sensitive to private key and nonlinear chaotic mapping can be used to add more randomness to the key generation process.

Table 2.1 Generation of Biometric keys

2.5.1 Symmetric Biometric Keys

In case of symmetric biometric keys, same biometric key is required at transmitter end and reception end as well. The various biometrics that are used now a day's as keys are fingerprint, iris, handwritten signature, voice, face, palm print etc. Initially, the biometrics is scanned by the owner himself and then that stored biometric patterns are compared with currently scanned biometric for further processing. There several applications are iris can used as locker's key, for computer login, forensics, anti-terrorism at borders for security reasons etc. The fingerprints are used as key the several android phones or Apple phones for the security of information stored in the cell phones. Recently, in 2015 China has developed tested ATM in which face of the person is recognized to withdraw money from the ATM to prevent fake withdrawals [72]. So, in this way the use of symmetric biometric keys is made for the security purposes. This thesis proposed for image encryption using symmetric biometric keys (i.e. combination of iris and fingerprint).

2.5.2 Asymmetric Biometric Keys

In asymmetric keys, pair of keys is used for encryption algorithm, public key is applied for encryption process and private key is required for the decryption purposes. To extract information from these types of keys both biometrics must be known to the hacker. In this thesis asymmetric keys are used for the video encryption. In asymmetric biometric key, the difference of biometrics is generated and used as key for encryption and decryption processes [16]. From transmitter side, the biometric of owner is sent and at the reception end biometric of receiver is scanned and then the difference of owner and receiver's biometric is taken and used as key for decrypting the video frame. So, use of these keys provides more protection and confidentiality to videos from the third parties. Instead of using single biometric, two biometrics are used (i.e. iris and fingerprint) for encryption procedure to reduces the chances of accessing key by deducing relation between the encrypted frames.

As discussed in literature, fractional transform and scrambling techniques used for the security purposes usually apply mathematical keys in encryption algorithms. Instead of using mathematical keys, biometric keys can be used in combination with fractional transform to enhance the security of existing techniques. For even better security, more than one biometrics can be used to enhance the quality of algorithms in combination with some other encryption technique. So, this prevailing need of security gives more encouragement to the invention of more complex algorithms.

2.6 MOTIVATION

Although several techniques are discussed in literature that are used for the security of images and videos, but in most of the techniques mathematical keys are used. The mathematical keys required space for the storage, because large keys cannot be memorized, so alternative solution is needed. To fulfill this requirement, biometric keys are introduced. These keys don't need storage; instead they are scanned to extract features for the generation from biometric keys.

Secondly, the use of fractional transforms has improved the performance of several applications, by providing an extra degree of freedom [29]. It attracts security systems, so many fractional transforms have been implemented for the encryption of images and videos, but still the use of modified fractional transform (like dual parameter based) is required for more improvement.

Another motivation is to enhance the performance parameters (like PSNR, MSE etc.) of existing techniques in order to provide better security to the images and videos from hackers.

As, discussed in literature the use of fractional transform and biometric keys in combination provides better results, so combination of more than one biometric can enhance the security to higher levels.

2.7 OBJECTIVES OF THE THESIS

This thesis acquires following objectives:

- To implement image encryption using DP-FrWT and scrambling in combination with symmetric multimodal biometric keys.
- To achieve ROI based video compression and encryption using DP-FrWT, scrambling and asymmetric multimodal biometric keys and its comparison with existing techniques.
- To compare proposed and existing image and video security techniques using quality parameters (like PSNR, MSE, SSIM etc.) and robustness from attacks.

CHAPTER 3

FRACTIONAL TRANSFORM AND SCRAMBLING

3.1 INTRODUCTION

The fractional transform belongs to family of linear transforms. It can change a function into any domain (i.e. frequency and time) [29]. The fractional transforms are used for the various applications because of increase in degree of freedom with the fractional orders; earlier the transform can use only integers as transform orders. There are several fractional transforms that are used now a day's such as FrFT, FrHT, FrMT, FrCT, FrWT etc. These transforms have several applications like time frequency analysis, compression, encryption etc. Further, this chapter introduced mathematical study of dual parameter based FrFT, dual parameter based FrWT and scrambling for encryption of images and videos.

3.2 FRACTIONAL TRANSFORM AND SCRAMBLING ALGORITHM

As discussed in literature, there was need of transform to improve the level of security techniques. Although, FT was used in many applications, but there were some constraints that create a gap to introduce some better transform with more degree of freedoms. So, FrFT comes into play in which number of transform orders are available between 0 and 1. To improve the performance of FT, wavelet transform (WT) was demonstrated and that too is extended further to get better results for numerous applications. Even now, WT was not sufficient to meet all the needs of modern world. After that combination of FrFT and WT invented new transform named as FrWT. The results of FrWT were even better to get more degrees of freedom to secure the information in better way. So, next section discussed the mathematical explanation about the DP-FrFT, DP-FrWT and scrambling methods used for the encryption od images and videos and for compression of videos in proposed algorithm.

3.2.1 Dual Parameter Based Fractional Fourier Transform (DP-FrFT)

The fractional transform is defined as the linear transformation in which definition of the transform is n^{th} power and n is not necessary to be an integer, thus it can transform images into any intermediate domain. The fractional transform is the basic transform that is used further to derive several transforms. The expression for single dimensional Fractional Fourier Transform is given as [7]:

$$F_g = \int_{-\infty}^{\infty} f(t) M_g(t,u)\, dt \tag{3.1}$$

$$M_{g}(t,u)=\begin{cases}\sqrt{\dfrac{1-j\cot g}{2®}}e^{i\left(\left(u^{2}+t^{2}\right)/2\right)\cot(g)-jut\,\mathrm{cosec}(g)} & \text{if } g \text{ is not multiple of } ® \\ ¢(t-u) & \text{if } g \text{ is multiple of } 2® \\ ¢(t+u) & \text{if } g+® \text{ is multiple of } 2®\end{cases} \quad (3.2)$$

where, $g = b®/2$ denotes angle of rotation in transform, $¢(t)$ is impluse function and b is transform order of matrix. The fractional Fourier transforms (FrFT) operator is designated as F_{g}. The visual evaluation of FrFT using a cosine signal is shown in Figure 3.1. To increase degree of freedom dual parameter based fractional Fourier transform (DP-FrFT) has been introduced, in which transform angle is also changed to increase level of security for the encryption process [7]. The development of DP-FrFT from FrFT provides better security to the information and makes the transform more complex that cannot be cracked very easily by the intruders. The mathematical expression for DP-FrFT is as follows:

$$X_{-}^{\sim} = Rm_{N}^{-}F^{\sim}(\mathrm{Rm}_{N}^{-})^{T}x \quad (3.3)$$

where, Rm is a rotation matrix, F is FrFT of the original image, x is original image, ~ is transform order, N is dimension of the rotation matrix, $^{-}$ is transform angle.

The expression for the inverse of DP-FrFT is given as follows:

$$x = Rm_{N}^{-}F^{-\sim}(\mathrm{Rm}_{N}^{-})^{T}X_{-}^{\sim} \quad (3.4)$$

Rotation matrix is used to enhance the security of fractional transform by changing its transform angle. The 2D rotation matrix is given as follows [7]:

$$Rm_{2}^{-} = Rm_{2} = \begin{bmatrix}\cos^{-} & \sin^{-} \\ -\sin^{-} & \cos^{-}\end{bmatrix} \quad (3.5)$$

Then 3D rotation matrix is given as:

$$Rm_{3}^{-} = Rm_{3} = \begin{bmatrix}1 & 0 & 0 \\ 0 & \cos^{-} & \sin^{-} \\ 0 & -\sin^{-} & \cos^{-}\end{bmatrix} \quad (3.6)$$

As it is well known that the need of better technique to improve efficiency is always encouraged, so further fractional wavelet transform has been introduced. The fractional wavelet transform was invented with combination of FrFT and wavelet transform in series to improve results.

3.2.2 Dual Parameter based Fractional Wavelet transform (DP-FrWT)

Wavelet transforms is defined as transform, for which wavelets are discretely sampled from mother wavelet by scaling and translating it in time intervals. This transform solved problem

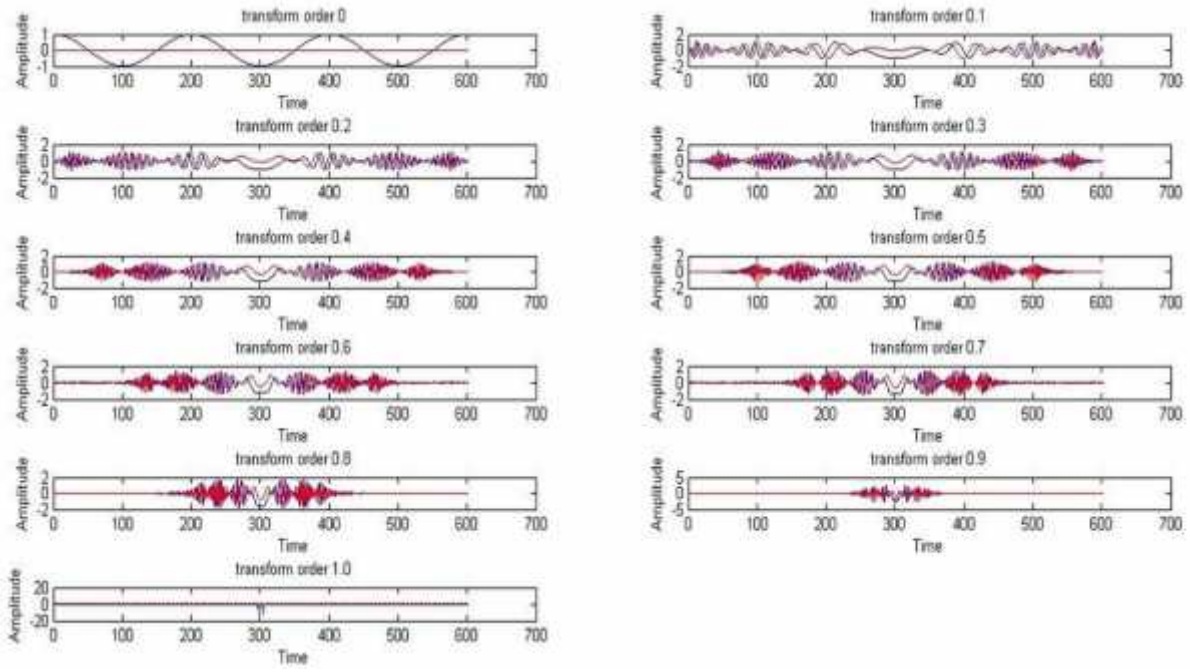


Figure 3.1 Visual representation of FrFT using cosine signal in different transform orders

faced in STFT. Mathematically, the mother wavelet function is represented as [73]:

$$\psi_{a,\tau}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-\tau}{a}\right) \tag{3.7}$$

Here, a and τ scaling and translation parameters of mother wavelet respectively, and t is time parameter. The mother wavelet has to satisfy the following conditions:

$$\int_{-\infty}^{\infty}\psi_{a,\tau}(t)\,dt = 0, \quad \int_{-\infty}^{\infty}\left|\psi_{a,\tau}(t)\right|^2 dt = 1 \tag{3.8}$$

Using Equation (3.3), the wavelet transform of input signal $x(t)$ is defined as:

$$F(a,\tau) = \int_{-\infty}^{\infty} x(t)\psi_{a,\tau}(t)\,dt \quad \text{ss} \tag{3.9}$$

Now inverse of fractional wavelet is defined as:

$$x(t) = \frac{1}{C_\psi}\int_{-\infty}^{\infty} F_x(a,\tau)\psi_{a,\tau}(t)\frac{da\,d\tau}{a^2} \tag{3.10}$$

where, $C_\psi = \int_{-\infty}^{\infty}\frac{\left|\hat{\psi}(v)\right|^2}{|v|}dv$ and $\hat{\psi}(v)$ represents FT of $\psi(t)$. Here, one thing is worth noting that no basis function is present in FrWT, unlike FrFT. The fractional wavelet transform is (FrWT) further developed by cascading of FrFT and wavelet transform.

The mathematical representation of continuous fractional wavelet transform is given as:

$$X_\psi(a,\tau) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x(t)K_\psi(t,y)\psi_{a,\tau}(y)\,dt\,dy \tag{3.11}$$

where, ~ is transform order, $\ddot{}_{a,²}(y)$ is the mother wavelet form and $K_{\sim}(t,y)$ is kernel of FrWT is given as:

$$K_{\sim}(t,y) = C_{\sim} k_{\sim}(t,y) e^{-ity\csc\tilde{}} \tag{3.12}$$

So, the inverse continuous fractional wavelet transform is:

$$x(t) = \frac{1}{C_{\ddot{}}} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} X^{\sim}(a,²) K_{\_\sim}(t,y) \ddot{}_{a,²}(y) \frac{dad² dy}{a^2} \tag{3.13}$$

Thus, forward discrete fractional wavelet transform (DFrWT) is given as:

$$X^{\sim}_{a,b} = \int F(x) \ddot{}_{a,b}(x) dx \tag{3.14}$$

where, a and b are integers used as a controlling factor for scaling and translation respectively.

The inverse discrete fractional wavelet transform (DFrWT) is given as:

$$F(x) = \sum_{a=-\infty}^{\infty} \sum_{b=-\infty}^{\infty} \left\langle F, \ddot{}_{a,b} \right\rangle \ddot{}_{a,b}(x) \tag{3.15}$$

The visual assessment of FrWT using a cosine signal is shown in Figure 3.2. The visual representation of FrWT and FrFT using cosine signal assures about more randomness in the signal of FrWT than FrFT. So, dual parameter based fractional wavelet transform (DP-FrWT) is further advanced version of FrWT is used in this work. In this transform, both transform order as well as transform angle are used as key to encrypt the images and videos. The mathematical expression for DP-FrWT is same as given in Equation (3.3). The expression for the inverse of DP-FrWT is given in Equation (3.4).

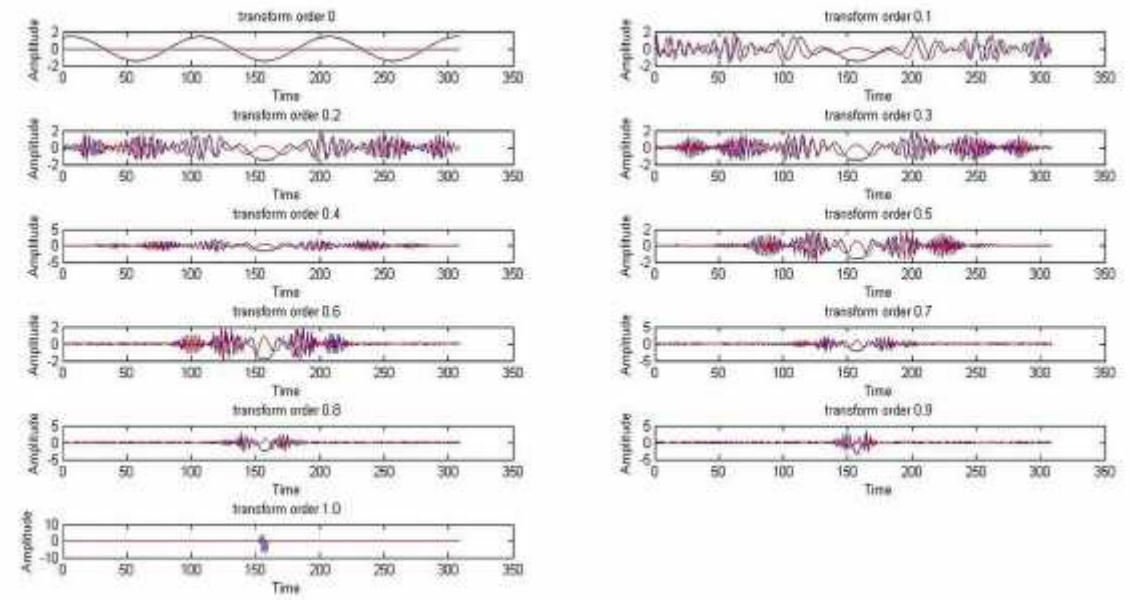
There are many methods that are available for the security purposes, but one of the simple is scrambling. It is discussed further and used to add more randomness in the encryption process, to create chaos in the images and videos, in combination with fractional transforms.

3.2.3 Scrambling

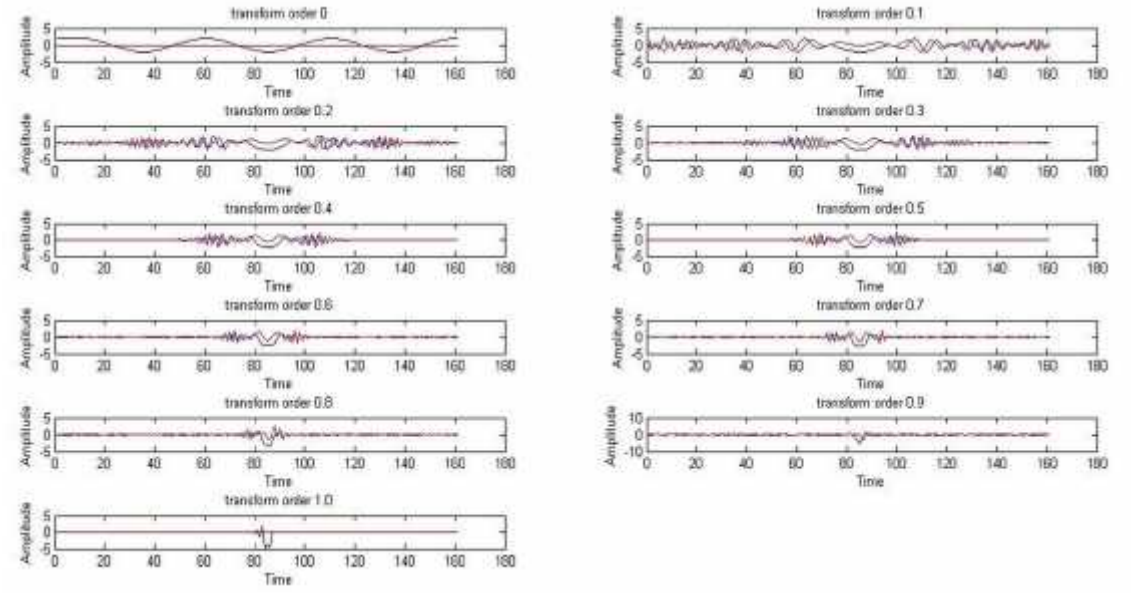
Scrambling is defined as a process of interchanging pixels of the image with each other in order to create chaos in the image [15]. This is also one of the algorithms that are used for image encryption. This is considered as one of the easiest method to create confusion in the actual data. To implement 2D scrambling on the digital image, initially the image is converted into a single column vector using:

$$V_f = \mathrm{Img}\, 2Vec(F) \tag{3.16}$$

where, V_f is vector generated from 2D image (F), is of size $M \times N$.



(a)



(b)

Figure 3.2 Visual representation of FrWT (a) Approximate coefficients (b) Horizontal coefficients

Now equation given below is used to generate random sequence:

$$S = rand(\mathrm{n}_e, \mathrm{X}) \tag{3.17}$$

where, X is the original image, n_e is number pixels in generating random sequences. To perform random scrambling of vector, V_f two random sequences S_a and S_b are required of size V_f (i.e. $M \times N$). The rule of scrambling is given as:

$$V_f\left(S_a(j)\right) \leftrightarrow V_f\left(S_b(j)\right)\ j = 0,1,2.....M \times N - 1 \tag{3.18}$$

where, $\leftrightarrow$ represents interchanging of elements in sequences S_a and S_b.

For the descrambling of encrypted image, use same chain rule given in Equation (3.18) is used. After descrambling V_f' will be obtained and then reverse conversion is made to convert a vector into matrix use following equation:

$$F' = \text{Img}\,2\,\text{Vec}^{-1}\left(V_f'\right) \tag{3.19}$$

where, F' would be much closed to the original image. Hence, in this paper scrambling has been performed on images obtained after applying DP-FrWT on the image. These algorithms are used for several applications.

3.3 APPLICATIONS OF FRACTIONAL TRANSFORMS

Fractional transforms (i.e. FrFT and FrWT) are used for several applications in various aspects of real life. Most of the applications that are implemented using fractional transform are encryption [5-9] and compression [48]. This application is required for the security purposes in various fields of technology. Using this technique, chaos is created in the image to hide actual information present in the data as shown in Figure 3.3. The eavesdropper is not able to comprehend the information hidden in the encrypted form.

(a) (b) (c)

Figure 3.3 Example of Encryption Algorithm

The other application that demonstrates use of fractional transform is noise removing filter. The optimal filter for removal of noise is required to get noise free image. Although normal Fourier transform is excellent for noise removing which is constant throughout the image [74]. To get better results even for uneven noise FrFT algorithm is implemented. The example for the noise removal is given in Figure 3.4. Except for the denoising and encryption, multipath chirp signal separation is also one of the applications of fractional transforms [75].

Compression is also one of the applications of fractional transform, in which size of the image or video is reduced by removing redundant information. Due to decrease in the size of the video or images low bandwidth is required. hence transmission cost is reduced. The other algorithm discussed is scrambling which is used for security purposes. Scrambler is also known as Gaussian filter to remove Gaussian noise [41]. These are some applications of proposed techniques that are being used in several areas for different purposes as per the requirement of systems.

(a) (b) (c)

Figure 3.4 Example of Noise Removal Algorithm

3.4 SUMMARY

This chapter includes the mathematical study of fractional transform and scrambling techniques used for the various applications. The comparison of FrFT and FrWT using cosine signal represents the presence of more randomness in FrWT than in FrFT, which is required in the encryption of multimedia contents. This encourages the use of fractional wavelet transform for the encryption of images and videos in proposed algorithm. It ended with the applications of the fractional transforms and scrambling, which are demonstrated in different areas with the visual example of image processing applications.

CHAPTER 4

IMAGE ENCRYPTION USING FRACTIONAL TRANSFORMS AND SCRAMBLING WITH BIOMETRICS KEYS

Image encryption deals with the need of security that is increasing very rapidly, to keep the confidentiality and integrity of digital images. This algorithm protects misuse of digital images by transforming it into jumbled form. This chapter discussed about the image encryption using fractional transforms and scrambling with combination of multimodal biometric keys.

4.1 INTRODUCTION

In order to provide security from intruders, encryption creates more confusion and diffusion to the images and makes them unintelligible for the hackers. Till now, several techniques are invented in past decade as discussed in literature are used of the encryption purposes. This thesis wills discussed encryption using dual parameter based Fractional Fourier Transform (DP-FrFT) and scrambling, dual parameter based Fractional Wavelet Transform (DP-FrWT) and scrambling in combination with multimodal biometric keys. The mathematical study of these transforms has been conversed earlier in previous chapter.

The keys applied for encryption process are symmetric biometric keys. The biometric keys are chosen, to lessen the chances of hit and trail method to guess the key. The key used is symmetric biometric key that means same biometric is required to retrieve the image at other end. The reason for choosing symmetric keys is not specific; it can vary from symmetric keys to asymmetric keys according to the applications. The biometric keys are preferred due to their unique and untraceable nature. For image encryption in proposed work, the key is used generated by XORing iris key and fingerprint key.

This chapter further disclosed the comparison of fractional transforms (DP-FrFT and DP-FrWT) in image encryption and various parameters such as PSNR (peak signal to noise ratio), MSE (mean square error), SD (spectral distortion) and SSIM (structural similarity index measure) are calculated to check quality of encrypted and decrypted images. Then, effect of differential attacks and spoofing attacks has been demonstrated. The efficiency of proposed algorithm is computed from its performance parameters and its power of resistance to several attacks.

4.2 IMAGE ENCRYPTION USING FRACTIONAL TRANSFORM, SCRAMBLING AND MULTIMODAL BIOMETRIC KEYS

As discussed earlier, image encryption is introduced to protect images from the attackers. Although the use of fractional transforms provides an extra degree of freedom to the encryption algorithm, but the decision of biometric keys adds an extra degree of freedom to this. The proposed algorithm is given with block diagram as in Figure 4.1. The methodology that has been adopted for the image encryption using fractional transform is disclosed further. As shown in block diagram, initially biometric keys are generated from their extracted features. After that performed the XORing operation using both codes generated from keys. Then, fractional transform and scrambling process are performed on the original image to make it in disorganized form. To extract original image back from ciphered image, all operations are reversed at the destination side of communication.

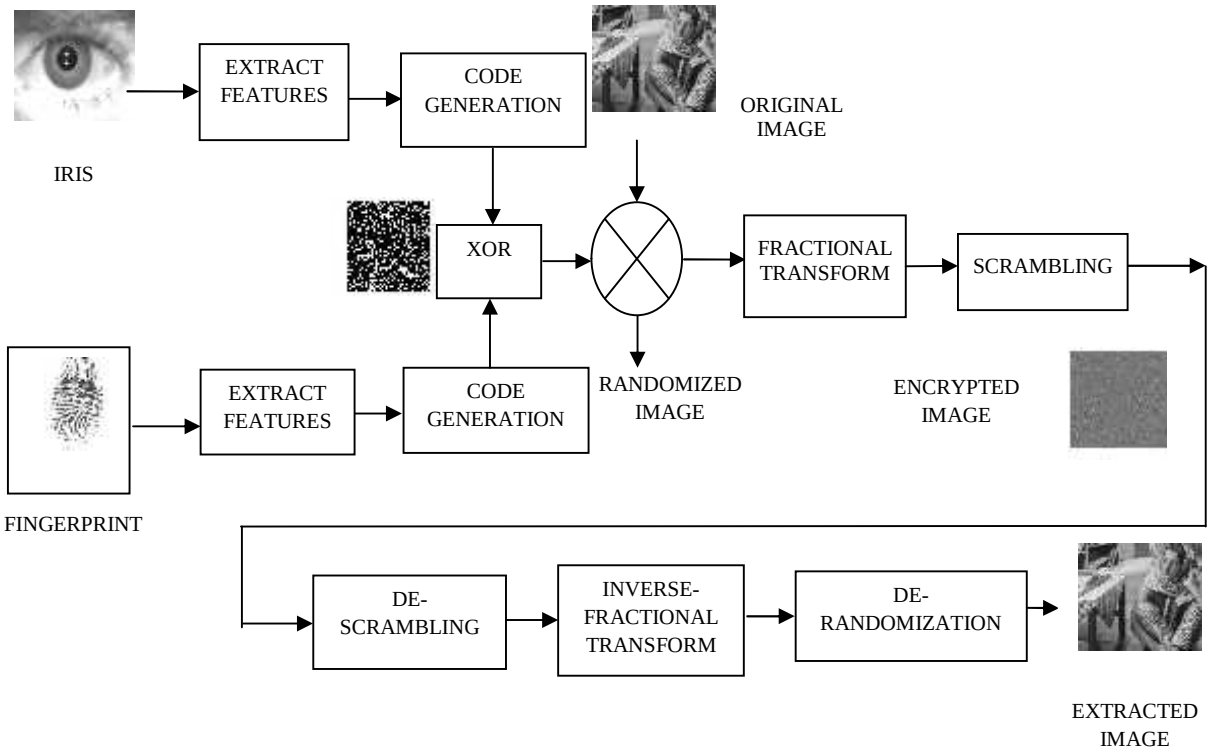


Figure 4.1 Block diagram of proposed algorithm

4.2.1 Biometric Key Generation

The keys used for encryption process are generated by taking scanned images of biometrics. Iris and Fingerprint are two biometrics used for the better security of the images in this thesis. The scanned images of iris and fingerprints are taken from the CASIA databases. Then, features of iris are extracted by using following steps:

- Detect iris and pupil from the scanned eye image using circular Hough transform.
- Then, iris is segmented from the other part of the eye.
- After extraction of iris, that biometric is denoted by $A=\left[a(\mathrm{m},\mathrm{n}):a(\mathrm{m},\mathrm{n})\in\left\{0,1,2,3.....2^{L}-1\right\}\right]$ having size $M_a \times N_a$, where M_a is size of columns and N_a is size of rows.
- Now, randomly select two pixels from the biometric denoted by p_1, p_2. Subtract these two values and divide it by total gray levels of biometric.

$$S=\left|p_1-p_2\right|/\left(2^{L}-1\right)\quad 0\le \mathrm{S}\le 1. \tag{4.1}$$

- Then, normalize that biometric image using

$$\tilde{A}=\frac{A-\min(A)}{\max(A)-\min(A)} \tag{4.2}$$

- Now generate feature matrix from the features of the iris using

$$F_A(\mathrm{m},\mathrm{n})=\begin{cases}1, \text{ if } \tilde{A}(\mathrm{m},\mathrm{n})\ge S\\ 0, \text{ if } \tilde{A}(\mathrm{m},\mathrm{n})< S.\end{cases} \tag{4.3}$$

where, S is calculated using Equation (4.1).

- The code is generated from that feature, denoted by $©_1$.
- Convert feature matrix into a feature vector, F_v and then breaks feature vector into two equal parts F_{v_a} and F_{v_b}. .
- To obtain, transform order and angle using segmented parts of feature vector is given as:

For transform order of x axis

$$_x=\frac{1}{M_a}\left[\left(\sum_{i=1}^{p/2}F_{v_a}(i)\right)\mathrm{mod}\left(2^{L}-1\right)\right] \tag{4.4}$$

For transform order of y axis

$$_y=\frac{1}{N_a}\left[\left(\sum_{i=1}^{p/2}F_{v_b}(i)\right)\mathrm{mod}\left(2^{L}-1\right)\right] \tag{4.5}$$

For transform angle of x axis

$$¤_x=\left(\sum_{i=1}^{p/2}F_{v_a}(i)\right)\mathrm{mod}180 \tag{4.6}$$

For transform angle of y axis

$$¤_y = \left(\sum_{i=1}^{p/2} F_{v_b}(i) \right) \bmod 180 \tag{4.7}$$

where, $\mathrm{mod}(\bullet)$ function is used to ensure value of transform angle between $[0,180]$ and transform order between $[0,1]$, L is length of feature vector, $p/2$ is the length of segmented parts of F_v .

Steps to generate code from Fingerprint

- The scanned fingerprint image is transformed into a binary image.
- Then thinning process is performed on that binary image, to reduce the thickness of fingerprint lines to single pixel width.
- Then extract minutiae of fingerprint from the thinned image of the fingerprint by finding ridges and bifurcation endings.
- From that ridge and bifurcations, the code is generated and is denoted by $©_2$.

After the generation of two keys $(©_1$ and $©_2)$, the original key $©$ is generated by XORing $©_1$ and $©_2$. Thus, the final key is ready to use in encryption process. After the randomizations of key with the original image, fractional transform and scrambling is applied successively on the randomized image is discussed in following sections.

4.2.2 Encryption and Decryption procedure

In the proposed block diagram, initially biometrics are taken to generate the key for the encryption of the images. The biometrics used is iris and fingerprint. The features of iris and fingerprint are extracted and then that extracted features are used for code generation. The generated codes are XORed to obtain the final key. Then as shown in Figure 4.1, the block diagram, final key and original image (that needs security) are randomized. After that, randomized image is processed further for the encryption process. After passing through the encryption procedure, the image is communicated in the open network for the communication with the receiver. Then, several attacks are applied by unknown authors to extract the information from the encrypted data. But this algorithm resists the attacks like NPCR (number of pixels change rate) And UACI (Unified Average Changing Intensity) in the open network. At the end, the receiver collects the information and applies reverse algorithms to extract the information. After that performance parameters like PSNR (peak signal to noise ratio), MSE (mean square error), SD (spectral distortion), SSIM (structural similarity index measure), correlation coefficients, histogram analysis and entropy are calculated to show the

improvement in proposed algorithm in comparison with existing algorithms. The key space analysis is made to check the resistance of algorithm from brute force attacks.

Steps for Encryption and Decryption process

- Firstly, the biometric key ($©$) and original image (I) must of same size $M \times N$. $©$ and I are randomized using formula:

$$R(m,n) = \frac{\ln\left(©(m,n)\right)}{\ln\left(I(m,n)\right)} \tag{4.8}$$

- After randomization, fractional transform is performed.
- Then scrambling is applied.
- Finally, the image is encrypted. For the decryption, descrambling is proceeded by decryption using inverse fractional transform.
- After decryption, de-randomization is performed to obtain the original image.

In this way, the images are encrypted before sending through the communication channel and then decrypted to get the original information from them. The encryption algorithm is applied on the gray images of size 480×480 as shown in Figure 4.2. The fractional orders $\sim_x$ and $\sim_y$ of the fractional transform (DP-FrFT or DP-FrWT) are decided using features of iris which varies as $[0,1]$. The encrypted images, decrypted images with incorrect keys and decrypted images with all right keys for some test images are shown in the Figure 4.3-4.7. This representation gives idea about the change in encrypted data with incorrect and correct keys, so that algorithm can be made strong enough to protect data from hackers.

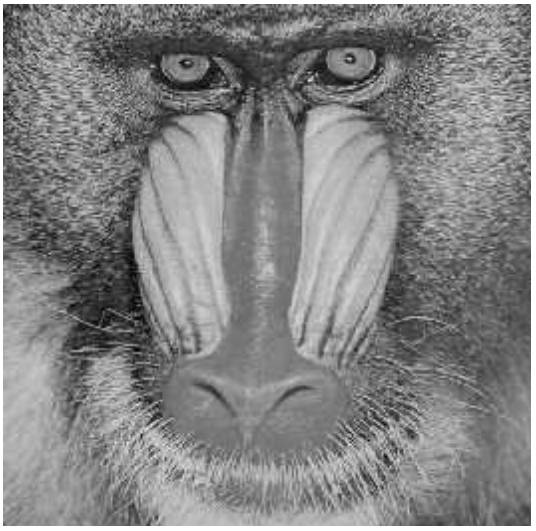
After that, visual representation of encrypted images, quality parameters (i.e. PSNR, SD, MSE, SSIM and entropy etc.) and attacks (i.e. differential attacks and spoofing attacks) are discussed. The visual representation of histogram analysis signifies about the chances of prediction of information from the encrypted images, if intensity of gray pixels is uniformly scattered, no information will leak through it. The evaluation of all these parameters helps to understand the faults in the algorithm, so improvement can be made in the algorithm for better results.

The discussion about performance parameters is need of every algorithm used for all the application, to check the efficiency of algorithm. So, the comparison of proposed algorithm with existing algorithms has been made with above mentioned performance parameters to show the improvement in results.

(a) Lena

(b) Barbara

(c) Cameraman

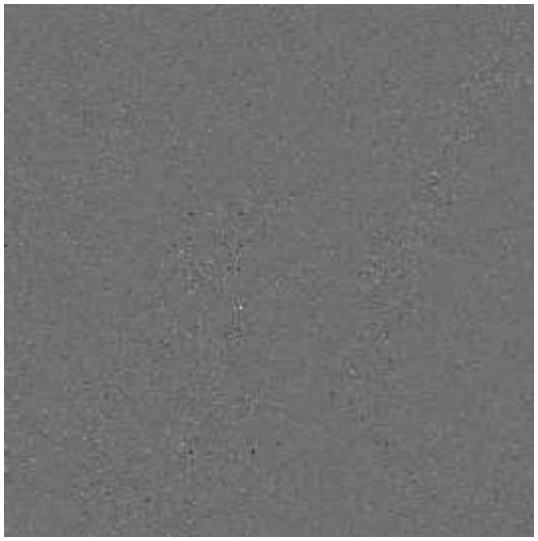


(d) Baboon

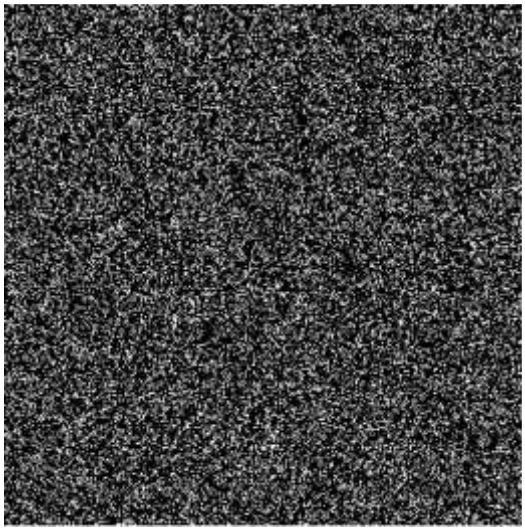
(e) Peppers

Figure 4.2 Test Images for Encryption

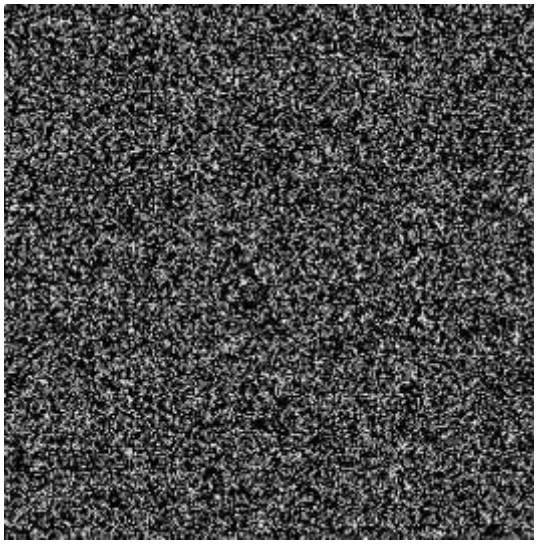
(a) Original Lena Image



(b) Encrypted Lena Image



(c) Decrypted with incorrect Biometric keys

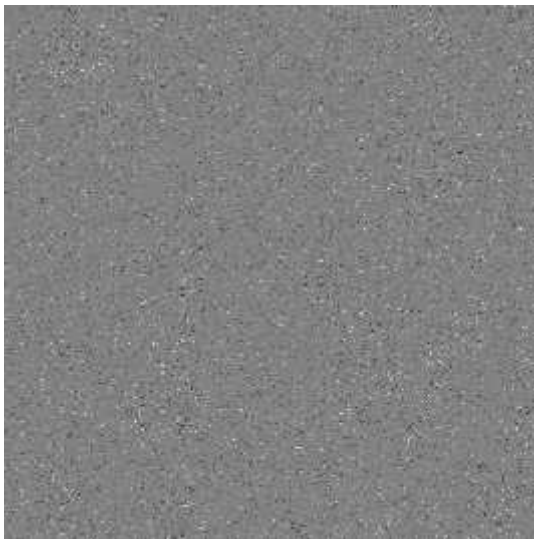


(d) Decrypted with incorrect Fractional order

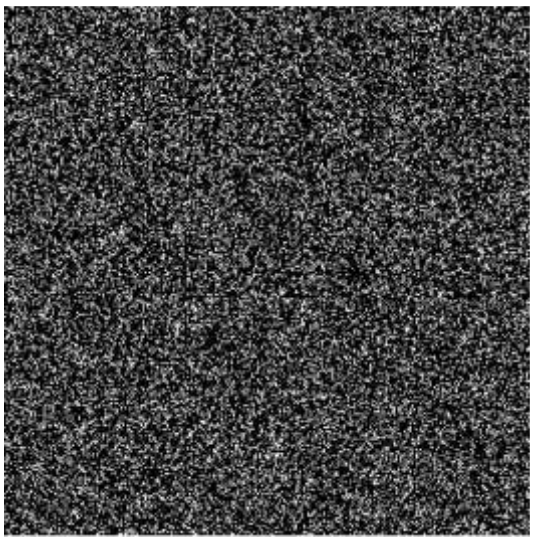
(e) Decrypted with all correct keys

Figure 4.3 Encryption and Decryption Simulation Results of Lena Image

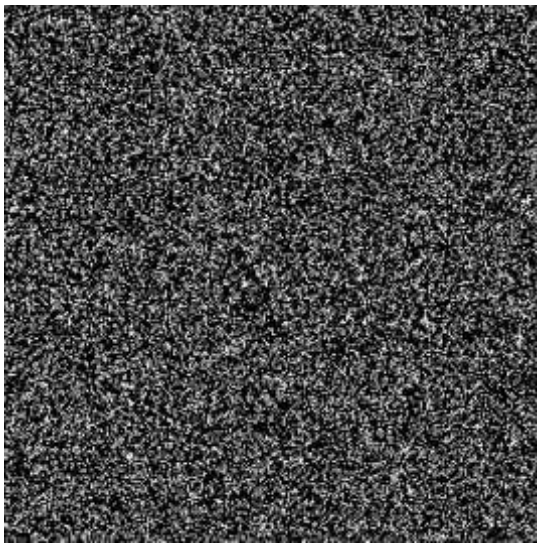
(a) Original Barbara Image



(b) Encrypted Barbara Image



(c) Decrypted with incorrect Biometric keys

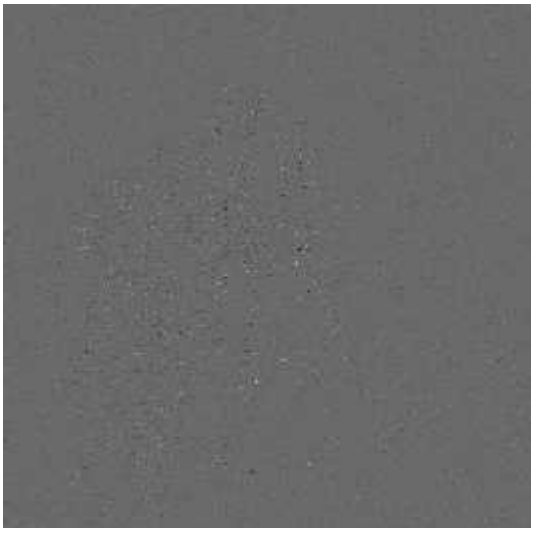


(d) Decrypted with incorrect Fractional order

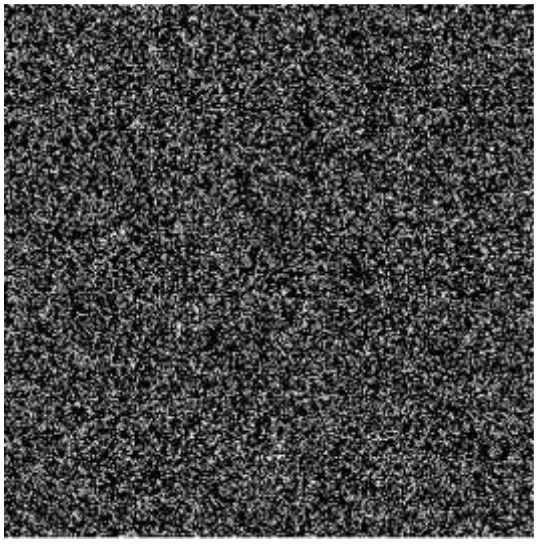
(e) Decrypted with all correct keys

Figure 4.4 Encryption and Decryption Simulation Results of Barbara Image

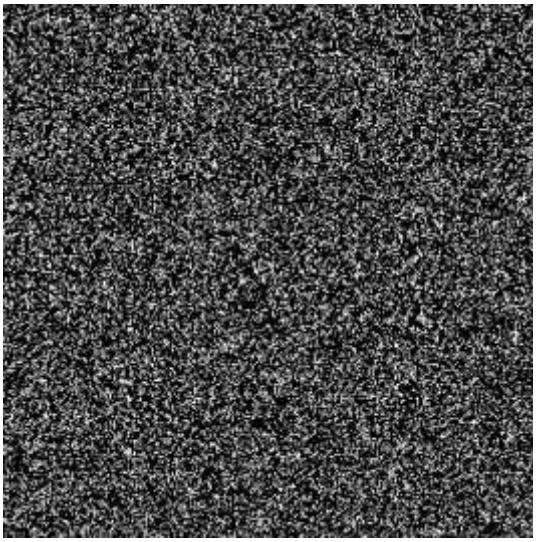
(a) Original Cameraman Image



(b) Encrypted Cameraman Image



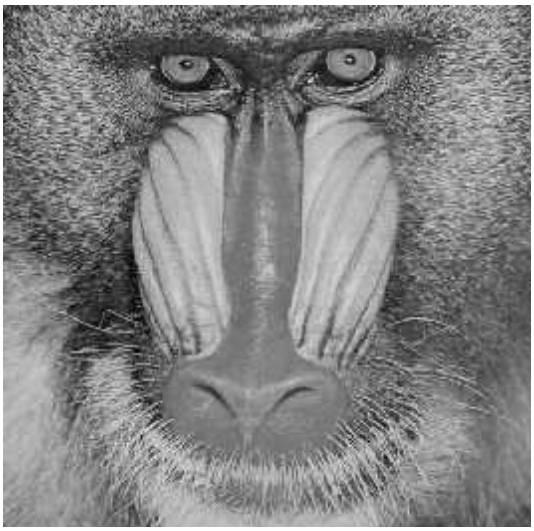
(c) Decrypted with incorrect Biometric keys



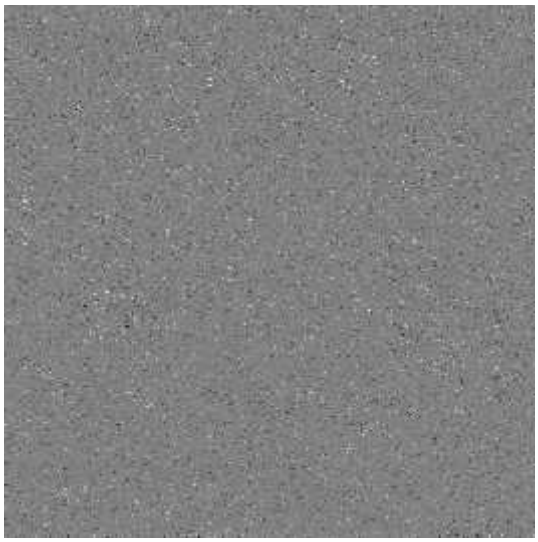
(d) Decrypted with incorrect Fractional Order

(e) Decrypted with all correct keys

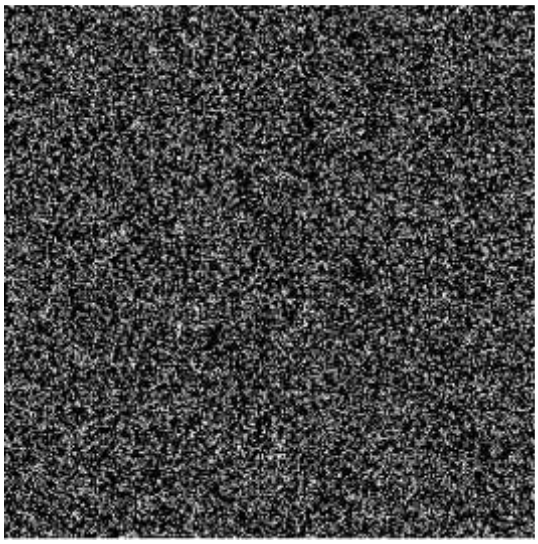
Figure 4.5 Encryption and Decryption Simulation Results of Cameraman Image



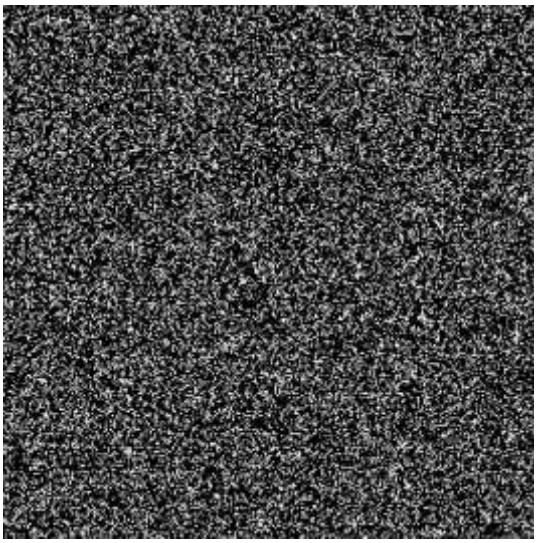
(a) Original Baboon Image



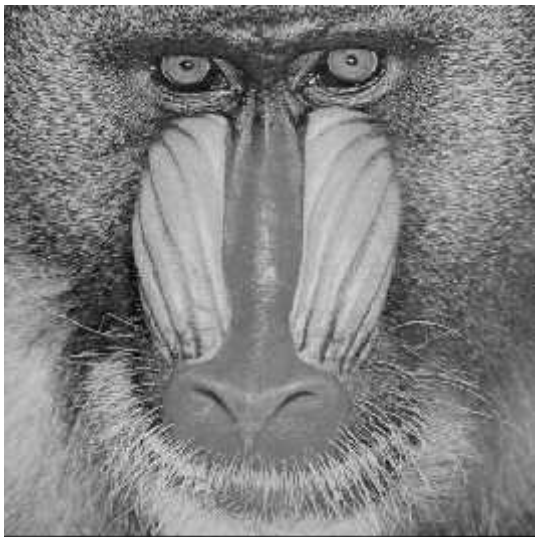
(b) Encrypted Baboon Image



(c) Decrypted with incorrect Biometric keys



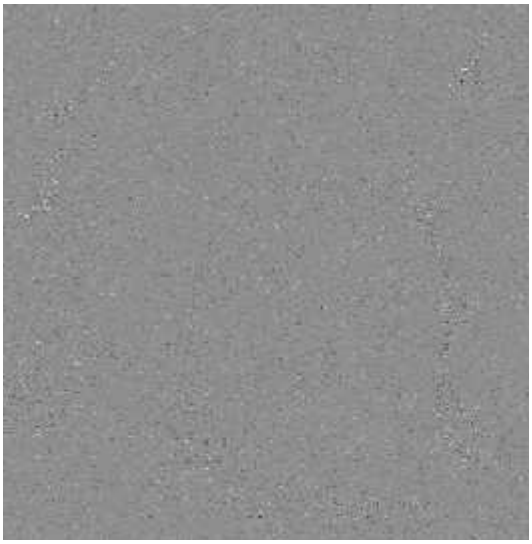
(d) Decrypted with incorrect Fractional order



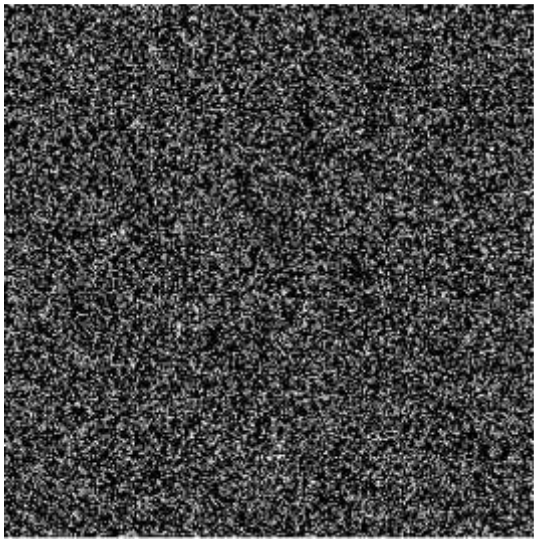
(e) Decrypted with all correct keys

Figure 4.6 Encryption and Decryption Simulation Results of Baboon Image

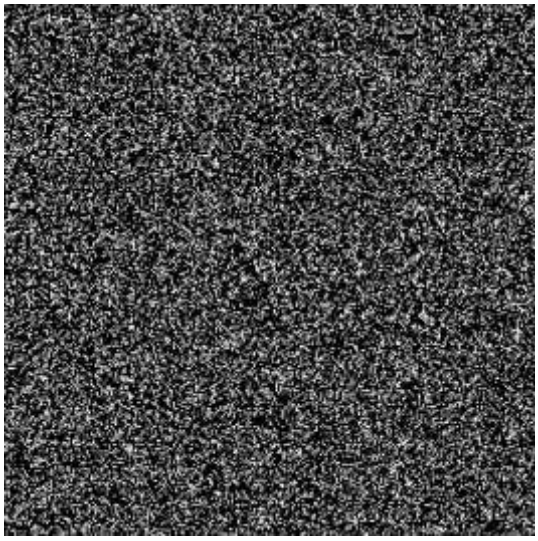
(a) original Peppers Image



(b) Encrypted Peppers Image



(c) Decrypted with incorrect Biometric keys



(d) Decrypted with incorrect Fractional order

(e) Decrypted with all correct keys

Figure 4.7 Encryption and Decryption Simulation Results of Peppers Image

4.3 PERFORMANCE ANALYSIS

After image encryption process several parameters are calculated to perform check security and visualization of encrypted and decrypted images. The perceptual security analysis and various statistical parameters are discussed as follows:

4.3.1 Analysis of Perceptual Security

The quality of the encrypted image is analyzed using various measurements, in order to receive good quality image at reception end. In this analysis, the parameters calculated are Peak Signal to Noise Ratio (PSNR), Spectral Distortion (SD), Structure Similarity Index Measure (SSIM) and Mean Square Error (MSE). All these parameters are calculated for comparing original, encrypted and decrypted images, to perform subjective evaluation of image arriving at receiver side. Further, all above parameters are discussed in detail.

PSNR represents the superiority of the signal that is retrieved from the randomized image after decryption image. It shows the amount of information present in extracted image with respect to noise. For perfect decryption of image its value must be close to infinity. The PSNR is given as:

$$PSNR(\mathrm{x},\mathrm{y}) = 10\log_{10}\frac{255^2}{\frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}\left(x_{m,n}-y_{m,n}\right)^2} \tag{4.9}$$

where, $x_{m,n}$ and $y_{m,n}$ are mn^{th} pixel of original and decrypted images respectively of size $M \times N$ The comparison of proposed technique and existing techniques has given in Table 4.1.

Images	PSNR					
	Proposed technique		DFrFT [48]	Scrambling [15]	DFrCT [76]	DCT + Arnold transform [77]
	DP-FrWT	DP-FrFT				
Lena	∞	∞	-	30.82	37.023	-
Baboon	∞	∞	60.08	-	-	13.4083
Peppers	∞	∞	-	-	-	10.1920

Table 4.1 Comparison of PSNR with existing Techniques

SD is used to determine spectral similarity between the actual and decrypted images. Its range should be close to zero. It is performed between original image and encrypted image to check

quality of encrypted image and it must be close to one [7]. The mathematical expression for SD is given as:

$$SD(x,y)=\frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}\left|V_x(m,n)-V_y(m,n)\right| \tag{4.10}$$

where, V_x and V_y are spectral values of originality and decrypted images or encrypted images. The comparison of existing techniques and proposed technique has given in Table 4.2.

SSIM is defined as measure to calculate structural similarity between original and decrypted images. Its range varies from $[-1,1]$. If the value is close to -1 then there is no similarity between images. If the value lies close to 1, then there is maximum similarity between original and decrypted images. The expression used is:

$$SSIM(x,y)=\frac{\left(2\mu_x\mu_y+D_1\right)\left(2\sigma_{xy}+D_2\right)}{\left(\mu_x^2+\mu_y^2+D_1\right)\left(\sigma_x^2+\sigma_y^2+D_2\right)} \tag{4.11}$$

where, x and y are actual and decrypted images respectively, D_1 *and* D_2 are constant to steady division with feeble denominator. The comparison of existing techniques and proposed technique has been compared in Table 4.2.

Images	Values Between Original and Decrypted Images	
	SD	SSIM
Lena	0	1
Barbara	0	1
Cameraman	2×10^{-5}	0.992
Zelda	0	1

Table 4.2 Security Analysis Parameters

MSE is defined as average of the error between original and decrypted images. It should be as low as possible. It represents the amount of error enters in the images while travelling through unprotected environment in original image with respect to reference image. Its value can be calculated as:

$$MSE=\frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}\left(I_x(m,n)-I_y(m,n)\right)^2 \tag{4.12}$$

where, I_x and I_y are original and decrypted images respectively. The MSE of proposed algorithm is zero. The comparison of MSE of proposed technique with existing techniques has given in Table 4.3.

Images	MSE			
	Proposed Technique		DFrFT [48]	FrFT [78]
	DP-FrWT	DP-FrFT		
Lena	0	0	-	0.05
Baboon	0	0	0.04	-

Table 4.3 Comparison of MSE with existing Techniques

All above parameters decide the quality of encrypted and decrypted images by analyzing mathematical values of PSNR, SD, MSE and SSIM. Further statistical parameters are discussed to examine statistical robustness.

4.3.2 Statistical Analysis

This analysis is computed to prevent leakage of information to invaders. The parameters that are calculated to determine statistical analysis are correlation between adjacent pixels of image and histogram analysis of original, encrypted and decrypted images. The visual representation of these parameters shows no similarity between pixels of encrypted images. These are discussed in detail as follows:

Correlation between adjacent pixels analysis is calculated to determine relation between pixels of original, encrypted and decrypted images. This shows the manner in which pixels of the image are related to their neighbor pixels. If they are closely related to each other, then value is close to 1. If its value approaches to zero, it represents uncorrelated pixels that are required in encrypted images. The correlation of the encrypted image must be less for good encrypted image. The formula for correlation (r_{ab}) is:

$$r_{ab} = \frac{E\left(a - E(a)\right)\left(b - E(b)\right)}{\sqrt{E\left(a^2\right) - \left[E(a)\right]^2}\sqrt{E\left(b^2\right) - \left[E(b)\right]^2}} \tag{4.13}$$

where, $E(a)$ and $E(b)$ are mean of adjacent pixels a and b respectively. $E\left(a^2\right)$ and $E\left(b^2\right)$ are variance of a and b respectively. The correlation of some test images has given in Table 4.4 along horizontal, vertical, diagonal and anti diagonal directions of images and their comparison with existing techniques is given in Table 4.5. It is observed that correlation between the pixel elements of encrypted images is low along vertical and diagonal directions, so it is protected from attackers. The visual representation of correlation between pixels is shown in Figure 4.8.

Images		Directions			
		Horizontal	Vertical	Diagonal	Anti-diagonal
Barbara	Original image	0.9237	0.9069	0.9190	0.9658
		Encrypted image			
	DP-FrWT	0.4997	-0.0064	-0.0018	-0.0022
	DFrFT	0.9988	0.0296	0.0297	0.0297
	Decrypted image	0.9237	0.9069	0.9190	0.9658
Zelda	Original image	0.9849	0.9924	0.9790	0.9807
		Encrypted image			
	DP-FrWT	0.4999	0.0020	-0.0012	0.1305
	DFrFT	0.9975	0.0730	0.0711	0.0711
	Decrypted image	0.9849	0.9924	0.9790	0.9807
Cameraman	Original image	0.9775	0.9881	0.9661	0.9696
		Encrypted image			
	DP-FrWT	0.4922	0.0028	-0.0013	0.0013
	DFrFT	0.9853	-0.0306	-0.0312	-0.0312
	Decrypted image	0.9743	0.9860	0.9630	0.9665
Pepper	Original image	0.9796	0.9824	0.9650	0.9676
		Encrypted image			
	DP-FrWT	0.4993	0.0048	0.0045	0.0048
	DFrFT	0.9990	0.0681	0.0679	0.0679
	Decrypted image	0.9796	0.9824	0.9650	0.9676

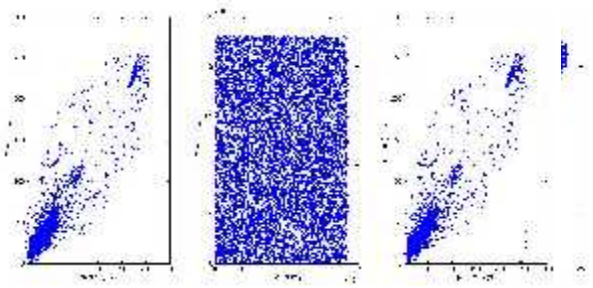
Table 4.4 Correlation between adjacent pixels of images

Images	Techniques	Horizontal	Vertical	Diagonal
Lena	Proposed Technique	0.5015	0.0020	-0.0010
	Fresnel Wavelet Transform[20]	0.0093	0.0086	0.0121
	DFrCT [76]	0.2261	-0.0607	0.0121
	MP-FrFAT [79]	0.0290	0.0270	0.0153
Baboon	Proposed Technique	0.5013	0.0030	-5.1504×10^{-4}
	Mellin transform[23]	0.1089	0.0878	0.0683
	Fresnel Wavelet Transform[20]	0.0077	0.0157	0.0092

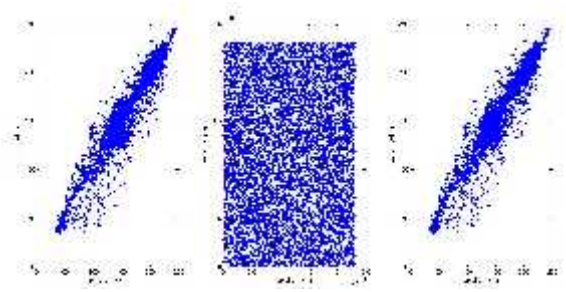
Table 4.5 Comparison of Correlation Coefficients between existing and proposed technique

The graph in Figure 4.8 represents uniform spreading of pixels in whole image after the encryption process to prove better encryption of the images. It is the requirement of good quality encryption to have uniform scattering of pixels to protect images from various attacks. In this way, due to scattering of pixels in whole image intruder won't be able to differentiate between encrypted image and any random noise. Even if hacker tries to calculate relation between adjacent pixels by making some changes nothing will come out of it.

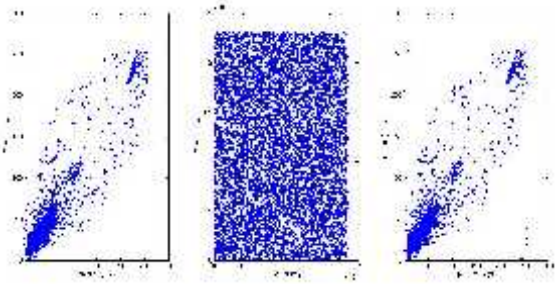
Histogram analysis is performed to evaluate distribution of gray pixels of original, encrypted and decrypted images in graphical form. For the superior quality encryption, the pixels should



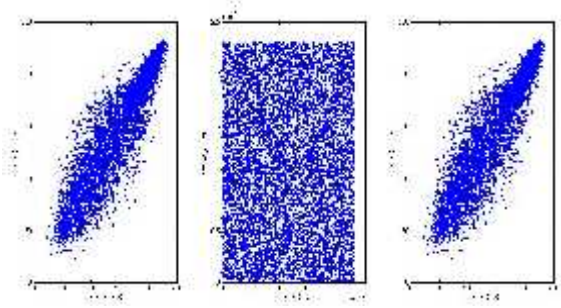
(a) Lena



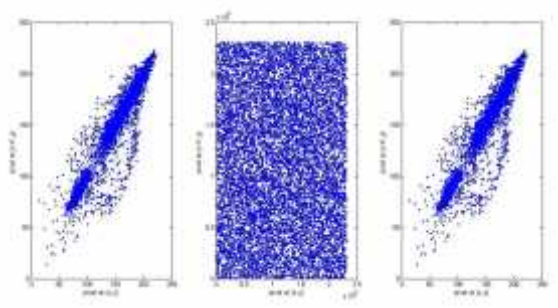
(b) Barbara



(c) Cameraman



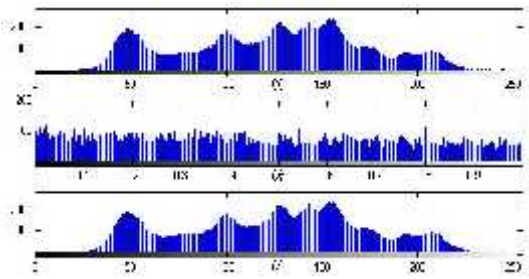
(d) Baboon



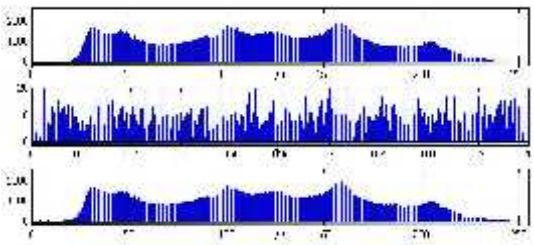
(e) Peppers

Figure 4.8 Correlation between adjacent pixels of actual, encrypted and decrypted images respectively

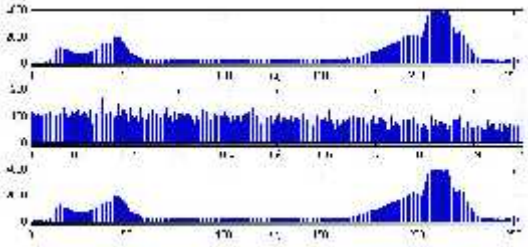
be distributed uniformly in the graph. The histogram analysis of test images predict that there is change in original and encrypted image that prevent escape of information, if attackers tries to extract relation between pixels of original image and encrypted image. The method used in this thesis provides uniform change in the distribution of pixels in image. The relation between the pixel elements of encrypted image is destabilized to the level that it is difficult for the intruder to calculate relation between pixels. The visual representation of histogram analysis is shown in Figure 4.9. It is observed form the Figure 4.9 that the pixels are uniformly distributed in encrypted image so it is free from histogram attacks. If intensity of all gray pixels of encrypted image is uniformly distributed than no predictions can be made to comprehend original information from it. Thus, without the information about the key used for the encryption no information will leak through it.



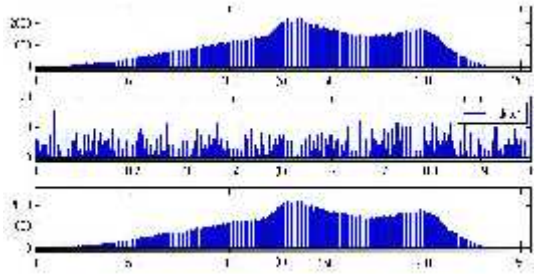
(a) Lena



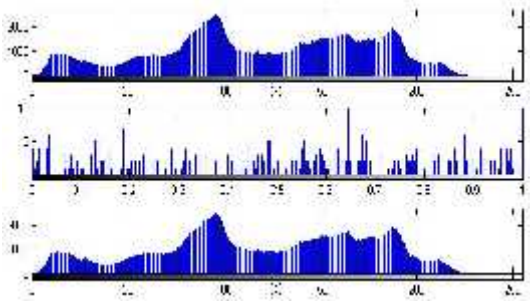
(b) Barbara



(c) Cameraman



(d) Baboon



(e) Peppers

Figure 4.9 Histogram representation of the actual image, encrypted image and decrypted image

4.3.3 Key Sensitivity Analysis

Key sensitivity is performed to check sensitivity of key that is used at the decryption side. If key used is exactly same that is used at transmitter side, then key sensitivity will be zero. Due to slight change in the key used for encryption, it will not decrypt the image at the receiver side. The keys used in the encryption process are transform order and transform angle of fractional transform that are generated from the features of iris key. So, if keys used at the decryption side are wrong, then it will not decrypt the image. The value of key sensitivity should be approaches to 100 for the better security of the image. The formula for the key sensitivity is given as [66]:

$$\mathrm{KS} = \frac{Dif\left(C1, C2\right)}{M \times N} \times 100\% \tag{4.14}$$

where, $M \times N$ is number of pixels in an image and $Dif\left(C1, C2\right)$ are given as:

$$\mathrm{Dif}\left(C1,C2\right)=\sum_{m=1}^{M}\sum_{n=1}^{N}C1\left(m,n\right)\otimes C2\left(m,n\right) \tag{4.15}$$

$$C1\left(m,n\right)\otimes C2\left(m,n\right)=\begin{cases}1, C1\left(m,n\right)\neq C2\left(m,n\right)\\ 0, C1\left(m,n\right)=C2\left(m,n\right)\end{cases} \tag{4.16}$$

where, C_1 and C_2 are decrypted images from correct key and incorrect key respectively. In this way, wrong key can be detected easily with sensitivity factor further another parameter for key security is size of key used to encrypt the images. The comparison of key sensitivity of proposed method with existing techniques has been given in Table 4.6. It is concluded from Table 4.6 that key sensitivity is large enough to detect the use of wrong key for encryption.

Images	Key sensitivity between decrypted image with correct key and incorrect key	
	Only fingerprint	Only iris
Barbara	84.3194	84.3194
Lena	84.3194	84.3194
Cameraman	84.1016	84.1984
Baboon	84.3190	84.3190

Table 4.6 Analysis of Key senstivity

4.3.4 Key Space Analysis

The analysis of key space is required to calculate the space of key that is used for the encryption process. It should be as large as possible for good encryption technique. In proposed method, key is generated using multimodal biometrics for the encryption process. For calculating the space of key, two sequences are generated using © and ©+$w$respectively © and© , having lengthT_1 . © $=\left\{0<h\left(g\right)<1\,|\,0<g<L_1\right\}$ and © $=\left\{0<\tilde{h}\left(g\right)<1\,|\,0<g<L_1\right\}$.

Formula for calculating mean absolute error is given as [66]:

$$M\left(\copyright,\copyright\right)=\frac{1}{T_1}\sum_{g=1}^{T_1}\left|\copyright\left(g\right)-\copyright\left(g\right)\right| \tag{4.17}$$

The key space is given as$\frac{1}{w_0}$, w_0 is given as value of w where, $M$is zero. After the calculation value of w_0 is 10^{-25}. So, key space for proposed algorithm is10^{25}, which is huge to protect information from brute force attacks. Even if, space of encryption is known to the intruder, he won't be able to extract actual key from it, because the biometrics used for the key generation have unique features that can't be guessed without the presence of original biometric at the reception end.

4.3.5 Entropy Analysis

Entropy of the encrypted image tells about chances of predicting encrypted content and it will create issue to the security of images. The entropy of good encrypted image should approaches to eight. If entropy is less that means there is chance of having threat to original image. The formula for entropy $H(x)$ is given as [39]:

$$H(x) = -\sum_{i=0}^{L-1} p(x_i) \log_2 \frac{1}{p(x_i)} \tag{4.18}$$

where, x is encrypted image, $p(x_i)$ is probability of x_i is i^{th} pixel of encrypted image. If value of entropy is closed to eight that means it is close to any random source. So, in this way it can be said that the information is unintelligible when in encrypted form. The comparison of entropy is given in Table 4.7. The above comparison table of entropy concluded the better results of proposed algorithm to defend against prediction of information from the encrypted images.

Images	Entropy (H)		
	Proposed technique		DCT + Arnold transform [77]
	DP-FrWT	FrFT	
Barbara	7.6166	3.7843	-
Lena	7.4434	3.7525	7.1796
Cameraman	7.0386	3.7825	-
Peppers	7.5865	3.8034	7.5521
Baboon	7.4699	3.6541	-

Table 4.7 Entropy Analysis

4.4 ATTACKS

Attacks can be defined as any type of attempt made to steal, modify, destroy or expose the information travelling through the channel. The attacks are generally made with wrong intention to break the confidentiality of information. Sometimes, attacks are also made for good reasons as well like call tracing to track terrorist etc. So, the attacks are also helpful in some areas, but to keep the information away from the intruders the encryption technique should be strong enough to resists them. The attacks are applied on the encrypted image to check the tolerance power of encryption algorithm from external attacks. The attacks include some differential attacks (like number of pixel rate change, unified average change intensity)on encrypted images and spoofing attacks on the biometric images used as the key in the encryption algorithm. So, in proceeding section these attacks are discussed in details to prove the resistance of proposed algorithm from several attacks.

4.4.1 Differential Attacks

The quality of image encryption is called excellent if it protects the digital images from attacks. In these types of attacks, trespasser makes minor changes in encrypted images and then tries to draw relationships between encrypted and original images to approximate original information. UACI (Unified Average Changing Intensity) and NPCR (Number of Pixels Change Rate) are calculated, in order to ensure no significant effect on the encrypted images with very little change. The parameters are discussed below:

4.4.1.1 NPCR

It is defined as rate of change of pixels of encrypted data. The expected value of NPCR is close to 100% to get highly encrypted images and for better security and the expression is:

$$NPCR = \frac{\sum_{m,n} D(m,n)}{MN} \times 100\% \tag{4.19}$$

$D(m,n)$ is given as:

$$D(m,n) = \begin{cases} 1, P(m,n) = \tilde{P}(m,n) \\ 0, otherwise \end{cases} \tag{4.20}$$

where, P and $\tilde{P}$ are two encrypted images. Here P is encrypted image of the actual image and $\tilde{P}$ is encrypted image of P which has one pixel change in it. The comparison of NPCR value of existing techniques and proposed technique has been given in Table 4.8 that concludes the defending of images from differential attacks. The high value of NPCR signifies the preservation of properties of encrypted images. The attacker tries to calculate the relation between two encrypted images, by changing single pixel, no leakage of information through it. The value of NPCR gives the idea of have differential attack on the encrypted image and sender will be alert to avoid the interference of any third party. In this way, NPCR plays very important role to defend encrypted information from the intruders.

Images	NPCR				
	Proposed Technique		FrFT over finite field[80]	Chaotic mapping [81]	DCT+FrMT [82]
	DP-FrWT	DFrFT			
Barbara	100	100	-	-	99.6496
Lena	100	100	98.5610	99.62	99.6698
Cameraman	99.9774	99.9583	-	-	-
Baboon	99.9996	99.9832	-	-	-

Table 4.8 Comparison of NPCR with existing techniques.

4.4.1.2 UACI

It is defined as the average changing intensity of the encrypted image with minor attacks. It is calculated by using:

$$UACI = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}\left|P(m,n) - \tilde{P}(m,n)\right| \times 100\% \tag{4.21}$$

where, P and $\tilde{P}$ are actual image and encrypted image. The value of UACI must be close to 33% for good encryption. The maximum value of UACI using proposed technique is 31.0174, which is enough to protect encrypted imaged from differential attacks.

4.4.2 Spoofing Attacks

Although biometric keys are good alternative to mathematical keys, but as the world is progressing in the field of technology, forgery of biometric keys is also possible. The biometrics are forged by several ways such as embedding iris features in contact lenses, creating gummy fingerprints, using face masks, etc. The detection of fake biometrics is performed using various methods, like checking frequency of ridges and edges, valleys and detection of pores in case of fingerprints [90]. In case of iris, the hamming distance (HD) between pixels of real and fake image is calculated. If HD is zero, then there is no spoofing attack, if it approaches the value 0.5 then the biometric is not original [91]. Instead of using different methods to detect falseness of different biometrics, general method is used where quality parameters [92] are calculated between input image and copy of that image after passing through Gaussian filter. To check spoofing attacks parameters like PSNR (peak signal to noise ratio), MD (maximum difference), SC (structural contents), MSE (mean squared error), LMSE (Laplacian MSE), TED (total edge difference), TCD (total corner difference), MAS (mean angle similarity), MAMS (mean angle magnitude similarity), JQI (JPEG quality index), SSIM (structural similarity index), GME (gradient magnitude error), GPE (gradient phase error), etc. are commonly calculated. The proposed algorithm has been given effective results while implemented on Galbally *et al.* [92] algorithm to check the spoofing attacks.

4.5 SUMMARY

Biometrics technology has enhanced the security of images when used as keys. The proposed algorithm used duo biometric keys i.e. iris and fingerprint for the encryption of images. Here, fractional transforms (DP-FrWT and DP-FrFT) and scrambling is used to add more randomness to the encrypted image. The proposed algorithm has infinite PSNR and zero

MSE as compared to the existing algorithms. The vertical and diagonal correlation coefficients of proposed algorithm are small in value from the existing methods. However, the comparison of DP-FrWT and DFrFT in terms of entropy concludes that DP-FrWT is better for image encryption than DP-FrFT . Key space analysis and UACI (Unified Average Changing Intensity), NPCR (Number of Pixels Change Rate), spoofing attacks ensure better security of ciphered image from external attacks.

CHAPTER 5

ROI BASED VIDEO SECURITY USING FRACTIONAL TRANSFORMS AND SCRAMBLING WITH MULTIMODAL BIOMETRIC KEYS

5.1 INTRODUCTION

Due to modernization in the world, the rate of data transferred through internet has increased. This work highlights the security of videos, transmitted through open network using several applications such as YouTube, whatsapp etc. The intruder can easily hack the information from the open channel and modify it before it reaches at the reception end. In order to protect the information from unauthorized persons, there is need of security techniques.

Recently used techniques for the partial video encryption are discussed in literature, to encrypt videos using perceptual based or ROI based encryption. In perceptual based encryption, the whole frame is partially encrypted. In ROI based encryption, only selected portion of frame is encrypted and rest of the frame is visible. Among several methods available for encryption, key encryption is very reliable. In this work, asymmetric biometric keys are used for encryption algorithm. Biometric keys are recommended because of their intractability and individuality.

This chapter proposed ROI based encryption for videos. Initially, the video frames are compressed. Compression is performed using DFrFT to reduce storage space and amount of bandwidth required for the communication from one end to other end. Then, after the compression is performed on selected portion and encryption is applied on it using DP-FrWT and scrambling with multimodal asymmetric biometric keys. The detailed explanation of proposed algorithm is discussed in further sections.

5.2 ROI BASED VIDEO ENCRYPTION

In this thesis the encryption performed on videos take face of person in videos as ROI, to hide the identity of person. As per requirement of application ROI can be chosen. The block diagram of proposed algorithm is given in Figure 5.1. In the block diagram the compressed frame of video is passed through the ROI selection process. After ROI selection, the randomization of ROI and biometric key (iris or fingerprint) is performed. Then, that randomized data is given to the DP-FrWT process and after that scrambling is applied to get actual ROI based encrypted video. Then that video is passed through the channel without

being affected by several attacks like ciphertext only attack, known plaintext attack etc. After that video is received at the reception end and reverse operations are performed on received video to get the original video. Further, algorithm is discussed to do ROI based encryption on videos. Initially, biometric keys are generated and then encryption process is applied on the videos. The results of video encryption are represented in Figure 5.3- 5.8 using some test sequences given in Figure 5.2.

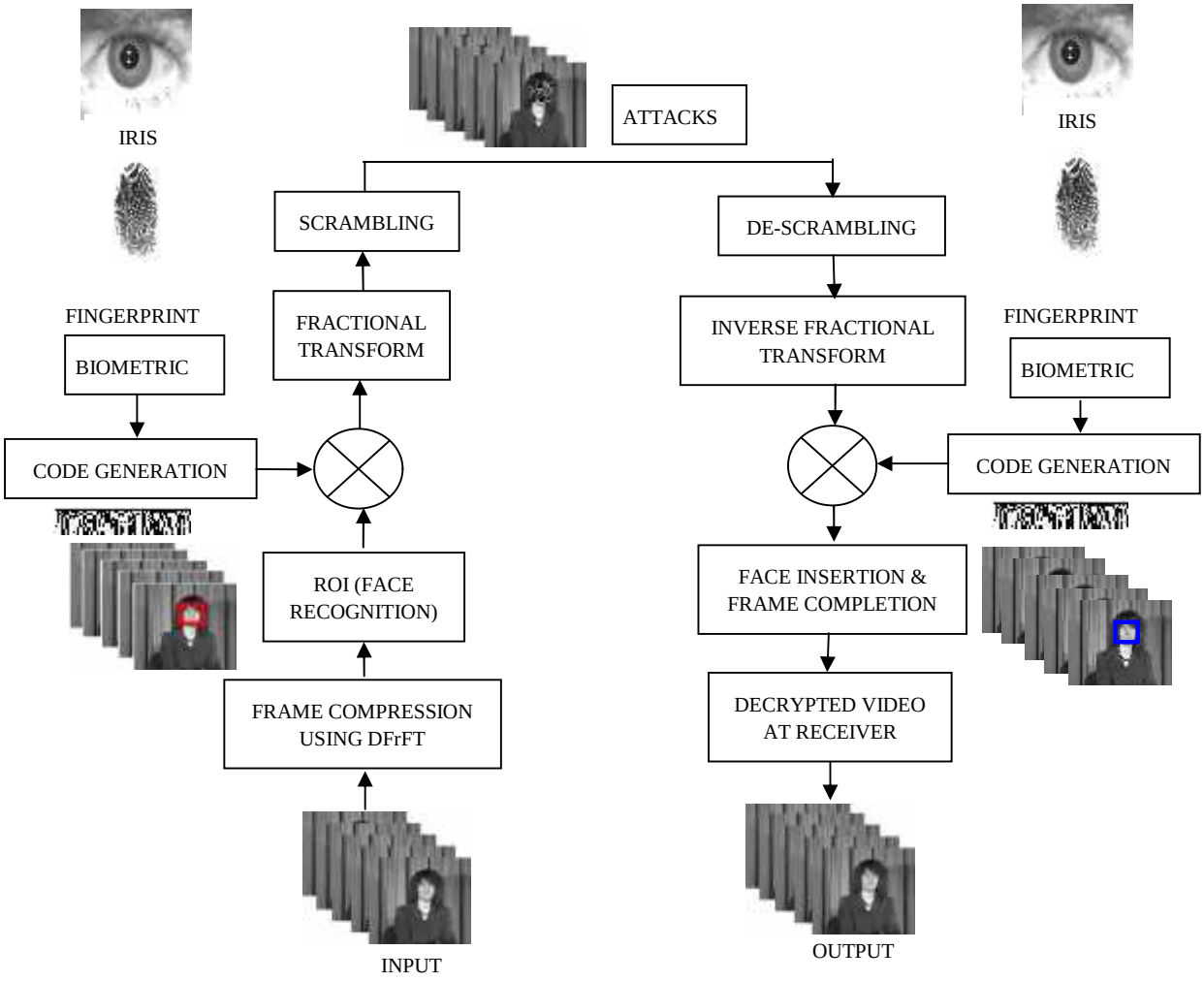


Figure 5.1 Proposed block diagram for ROI based video encryption

5.2.1 Generation of Biometric keys

For generating biometric key, scanned biometrics is used. In proposed technique, iris and fingerprint are used as biometric keys. The codes are generated using iris is denoted by $©_1$ and code generated using fingerprint is represented as $©_2$. Alternatively, both keys $©_1$ *and* $©_2$ are used for the encryption process to add an extra security to the procedure. Now, actual keys are ready to lock ROI of frame. To use these keys as asymmetric key, biometric of sender as well as biometric of receiver is used to generate key for single frame encryption. In this way

public key is transferred through network, while other half of key (private key) is scanned at reception end.

5.2.2 Compression

Compression is performed to reduce the amount of bandwidth required for the transmission of information through the channel [48]. Steps for the compression of video are:

- Initially the frame of video is extracted and divided into non-overlapped sub-blocks, generally used sub-frames are 8×8 and 16×16. In this work 8×8 blocks are used for the simulation results.
- Then, discrete fractional Fourier transform is applied on each block of frame with chosen compression ratio. By applying fractional transform the pixels are converted into transform domain coefficients.
- After that quantization is performed to eliminate the coefficients containing least information and further compression is performed using run length coding algorithm.
- At the other end, inverse of transform is performed to have the test video again in gray scale from.

Now, test videos are in compressed form and ready to proceed further for encryption.

5.2.3 Encryption and Decryption Algorithm

Here, region of interest (ROI) is chosen and encrypted to provide security. The ROI selected in is face of person in test videos, to hide the identity of person from the hackers. The steps for the encryption and decryption are as follows:

- Firstly, the biometric key (©) and ROI of frame (I) must of same size $M \times N$. © and I are randomized using Equation (4.8).
- After randomization, DP-FrWT is performed and then scrambling is implemented.
- Finally, the ROI of frame is encrypted. For the decryption, descrambling is proceeded by decryption using inverse DP-FrWT.
- After decryption, de-randomization is performed in order to obtain the actual video.

Thus encryption and decryption of videos is performed using DP-FrWT, scrambling and multimodal biometric keys. After the implementation, the performance parameters are calculated that decides the quality of encryption performed on the multimedia content. The attacks are also considered to resist the harmful effect on ciphered information while communicating through the open network.

(a) Akiyo

(b) Deadline

(c) Lady

(d) Grandma

(e) Claire

(f) Foreman

Figure 5.2 Test videos for ROI based encryption

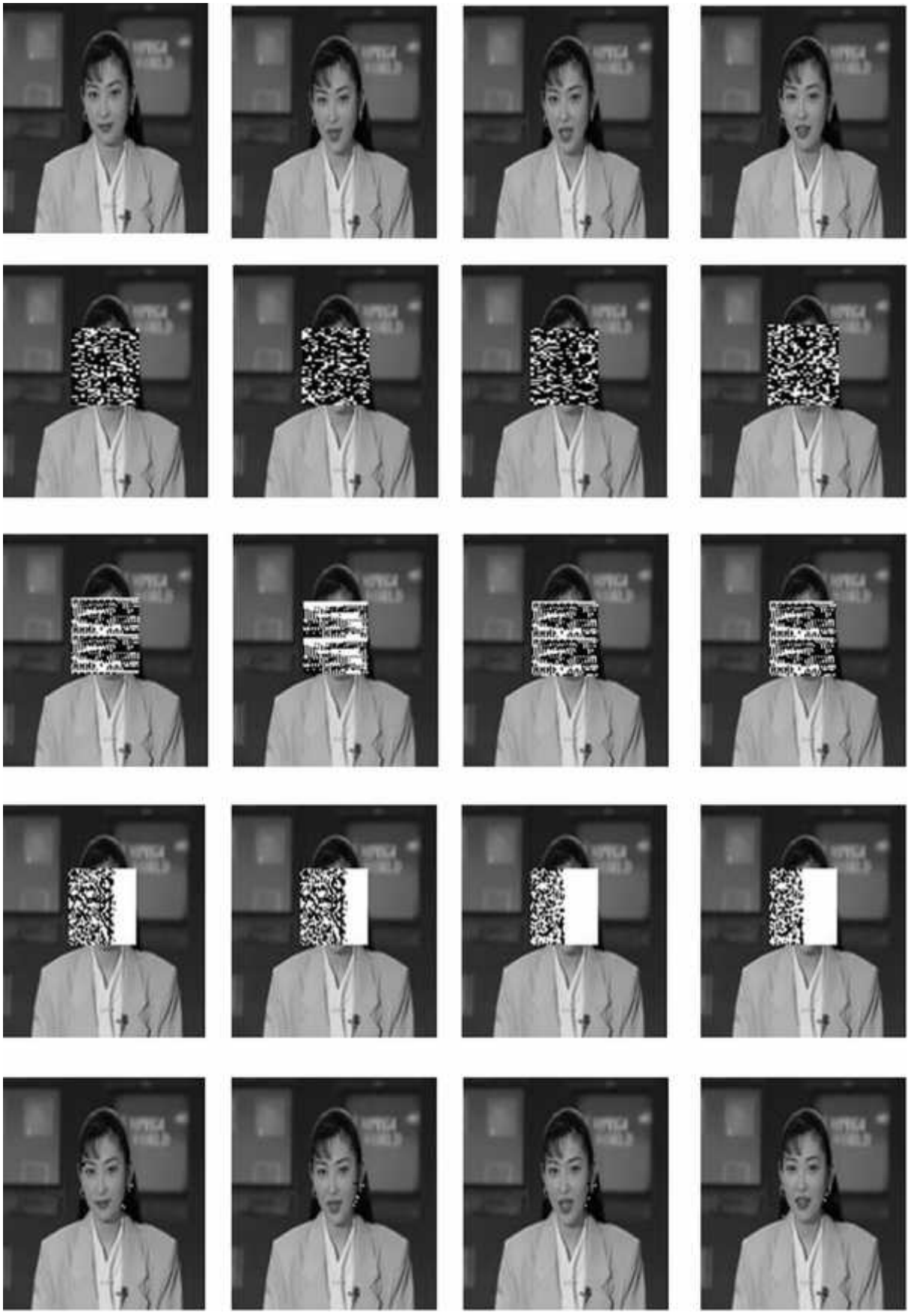


Figure 5.3 Visualization of ROI based encryption on Akiyo test video with frames 1, 11, 15, 24, First row-Original frames, Second row-Encrypted frames, Third row-Decrypted with wrong iris key, Fourth row-Decrypted with wrong fingerprint key, Fifth row-Decrypted with all correct keys

Figure 5.4 Visualization of ROI based encryption on Deadline test video with frames 31, 38, 49, 51, First row-Original frames, Second row-Encrypted frames, Third row-Decrypted with wrong iris key, Fourth row-Decrypted with wrong fingerprint key, Fifth row-Decrypted with all correct keys

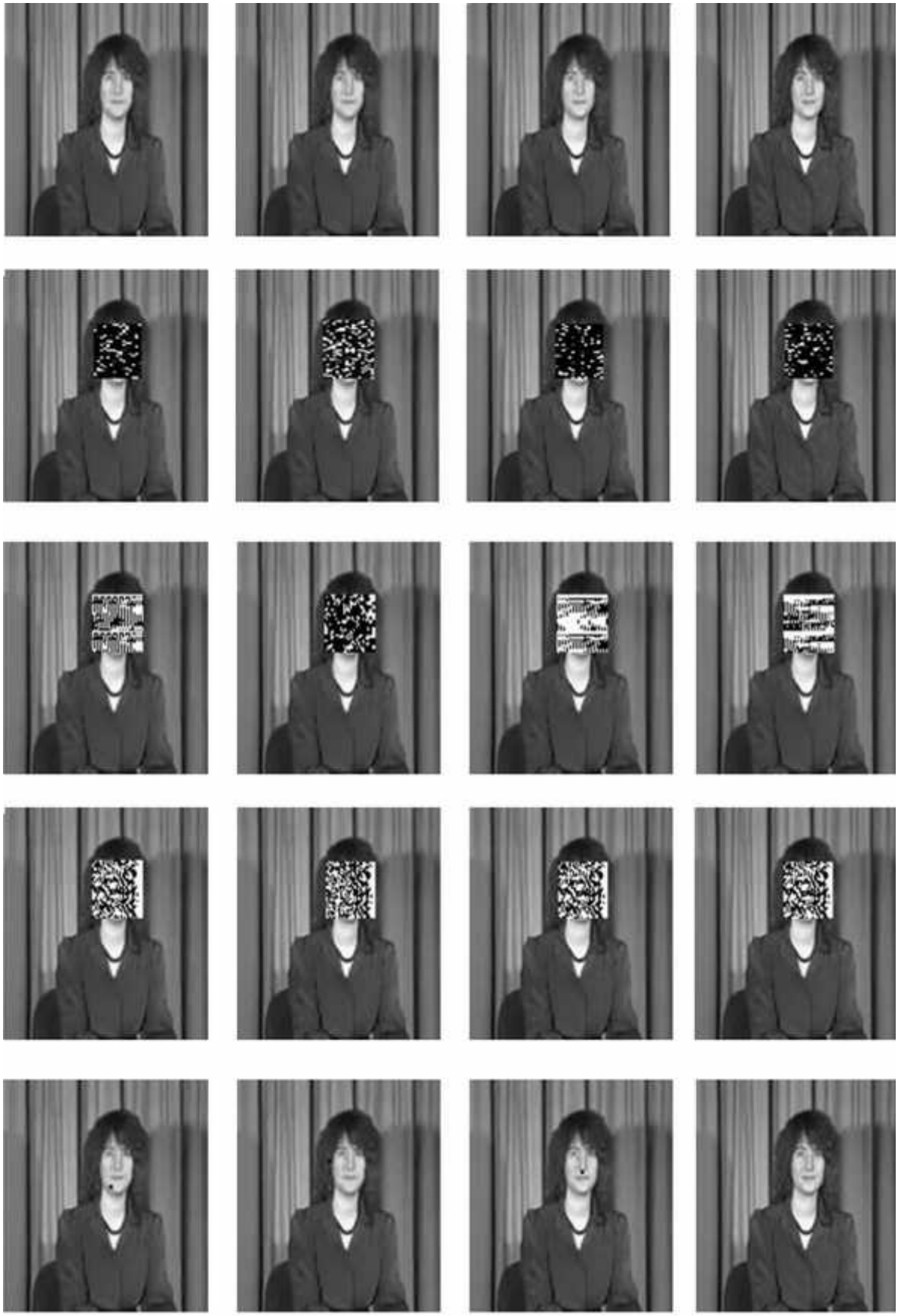


Figure 5.5 Visualization of ROI based encryption on Lady test video with frames 1, 8, 11, 24, First row-Original frames, Second row-Encrypted frames, Third row-Decrypted with wrong iris key, Fourth row-Decrypted with wrong fingerprint key, Fifth row-Decrypted with all correct keys

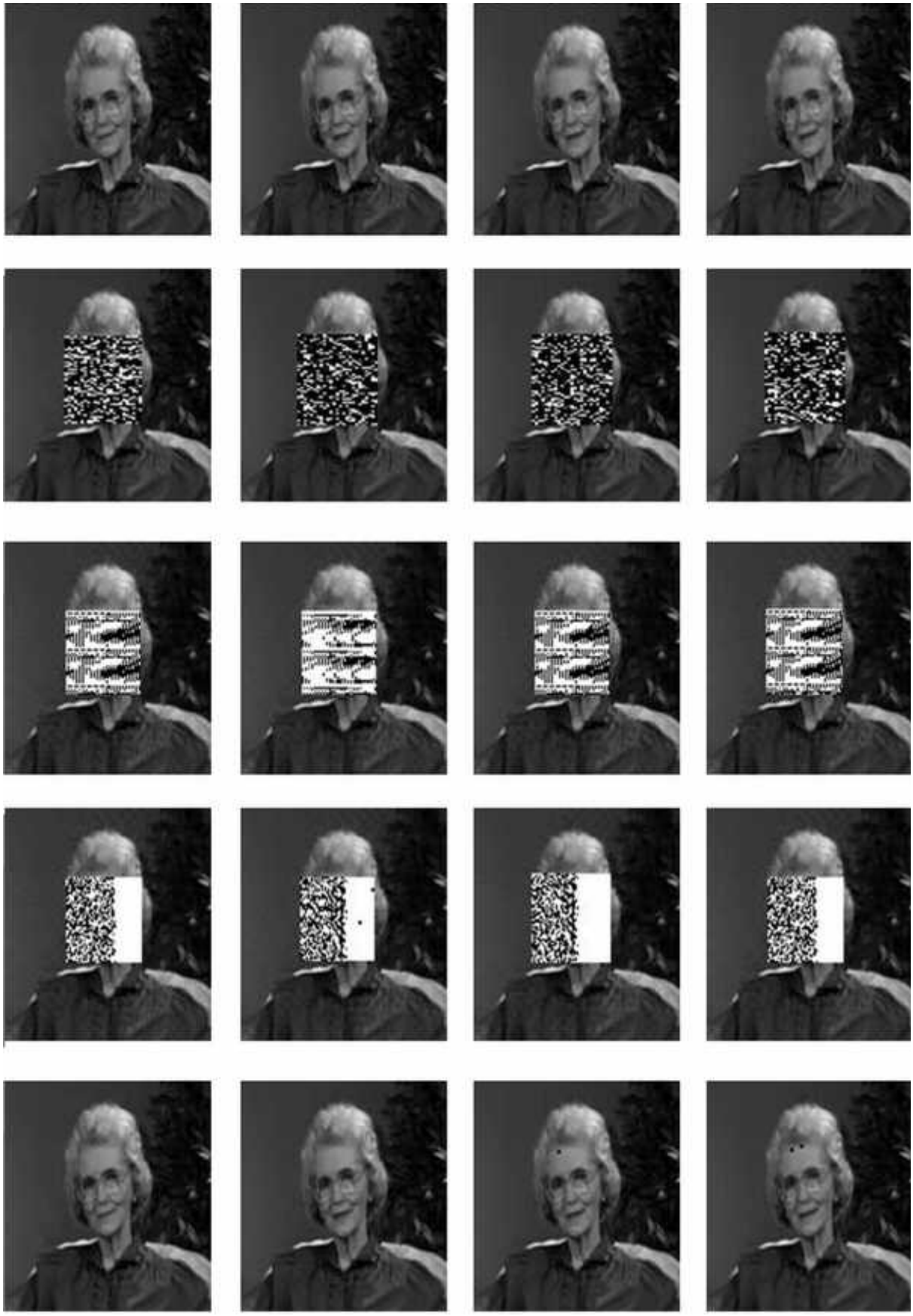


Figure 5.6 Visualization of ROI based encryption on Grandma test video with frames 9, 16, 19, 23, First row-Original frames, Second row-Encrypted frames, Third row-Decrypted with wrong iris key, Fourth row-Decrypted with wrong fingerprint key, Fifth row-Decrypted with all correct keys

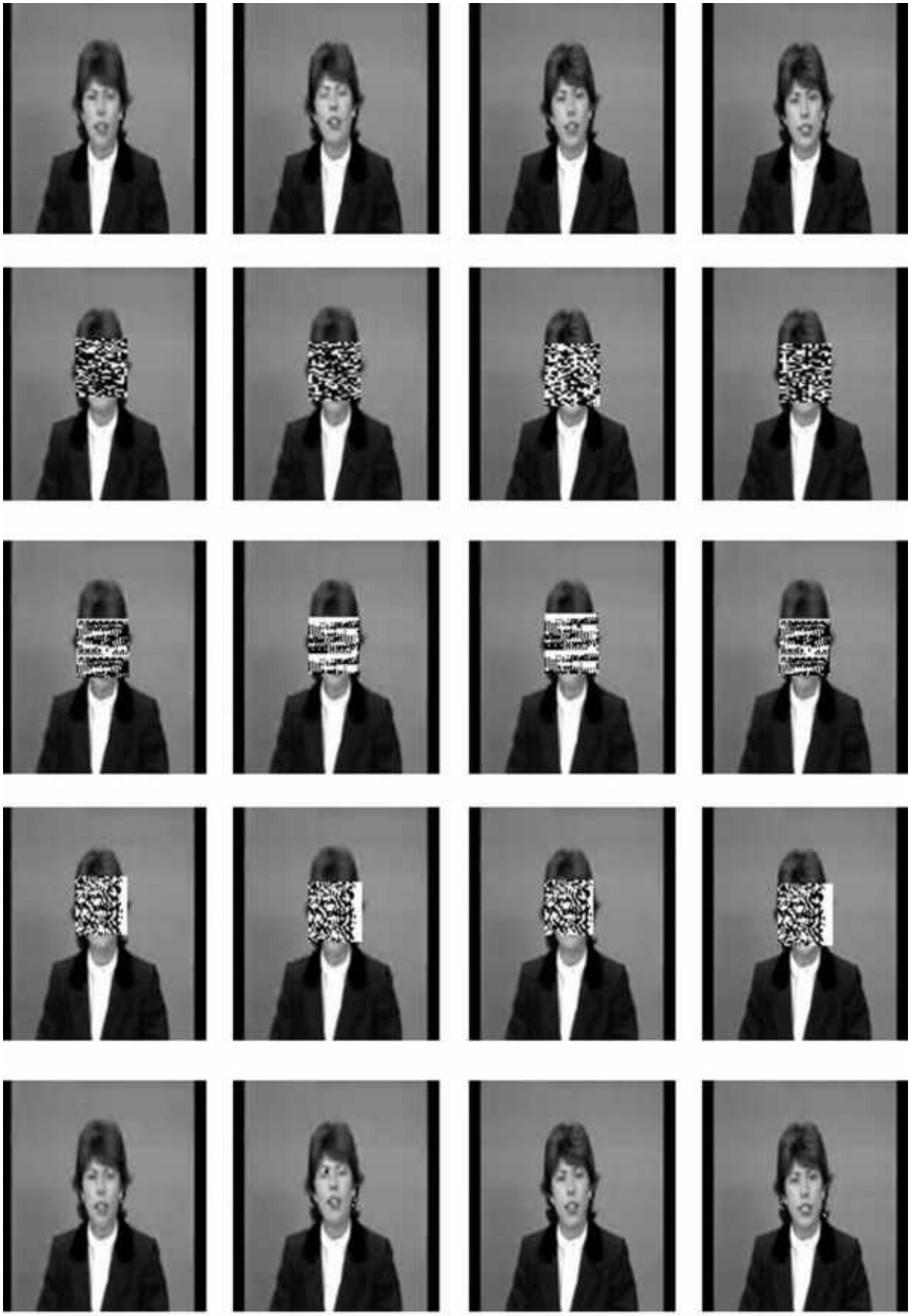


Figure 5.7 Visualization of ROI based encryption on Claire test video with frames 4, 10, 19, 22, First row-Original frames, Second row-Encrypted frames, Third row-Decrypted with wrong iris key, Fourth row-Decrypted with wrong fingerprint key, Fifth row-Decrypted with all correct keys

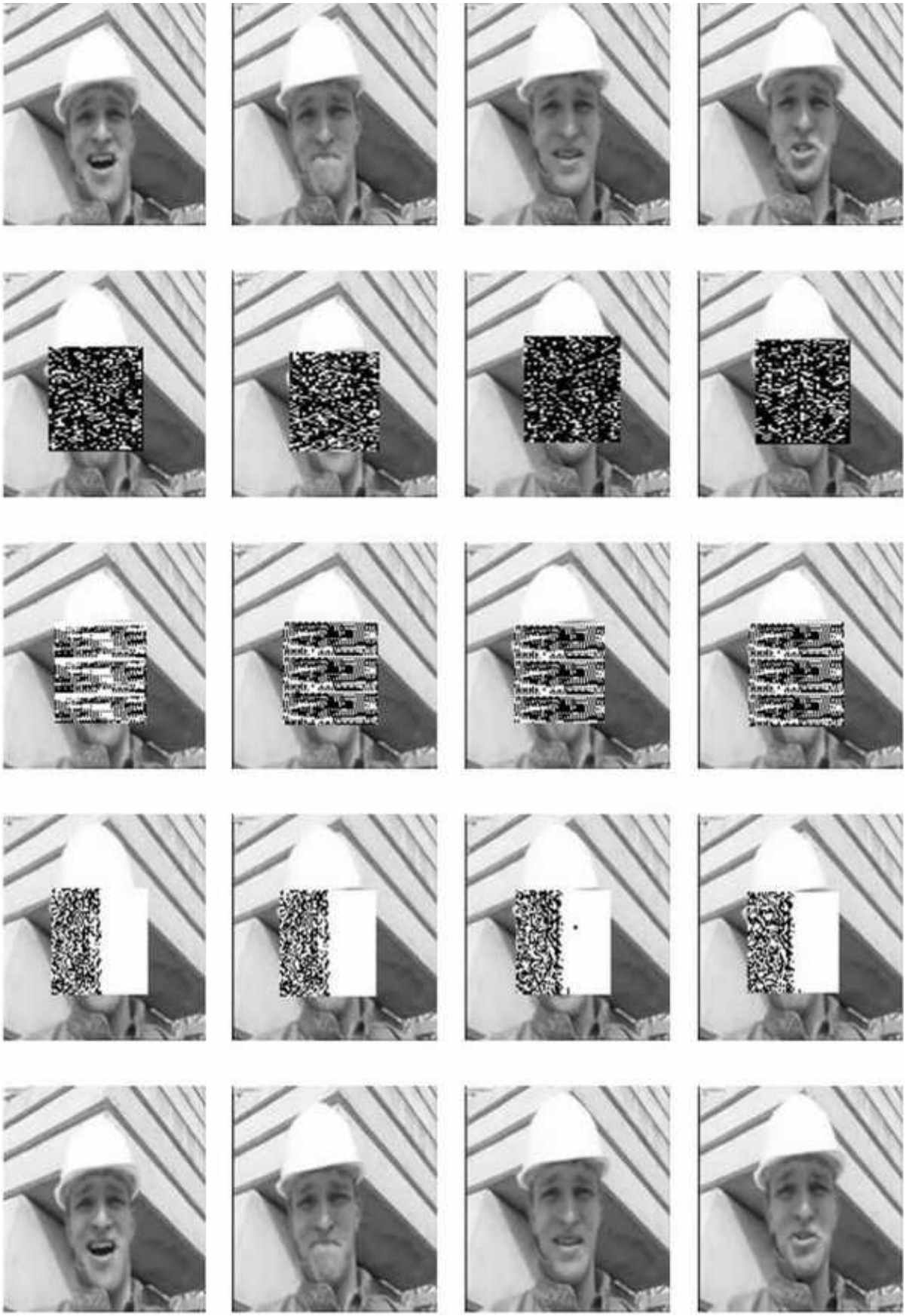


Figure 5.8 Visualization of ROI based encryption on Foreman test video with frames 30, 39, 48, 53 , First row-Original frames, Second row-Encrypted frames, Third row-Decrypted with wrong iris key, Fourth row-Decrypted with wrong fingerprint key, Fifth row-Decrypted with all correct keys

5.3 SECURITY ANALYSIS

The simulation tool used in proposed technique is MATLAB2013a. The gray scale videos like Akiyo, foreman, Claire, lady and grandma are considered for experimental results. In the proposed technique, keys used for encryption are asymmetric biometric keys (iris or fingerprint). The meaning of the security is that the ROI of video frame is in jumbled form and must not be recognized by any person. In search of enhancing the level of security encryption technique is proposed, in which the key is generated by using two biometric. The use of biometrics adds an extra degree of freedom along with fractional order and transform angle that provides better security. PSNR of test sequences is calculated to show quality of decrypted video received at the destination side with different compression ratios as given in Table 5.1. The observations has been made from the comparison table that there is decrease in PSNR ratio with the increase in CR. The PSNR of decrypted video with correct key, with wrong keys and without wrong key is represented through graph between PSNR and BPP (bits per pixel) in Figure 5.10

Compression Ratio	Video Sequences					
	Akiyo (352×288)	Deadline (192×144)	Lady (176×144)	Grandma (192×144)	Claire (176×144)	Foreman (176×144)
10%	53.9588	56.5632	57.4853	55.1935	57.1283	54.5438
20%	53.9826	52.3184	55.3240	53.7065	56.7102	50.1727
30%	51.8847	47.7482	53.9311	50.8980	53.6812	46.9322
40%	49.3707	45.5159	51.4895	49.0940	50.4211	43.4557
50%	46.1893	41.7334	47.4471	45.7033	48.1467	40.4686
75%	37.5550	34.6149	38.0661	38.4329	38.4322	32.9113

Table 5.1 Average PSNR of test videos

It is observed from the bar graph shows the improvement of 3dB PSNR of proposed algorithm in comparison with existing algorithms. This proves the better efficiency of proposed algorithm. The graph between PSNR with BPP (bits per pixel) represents the change in PSNR of video with the variation in compression ratio. BPP is defined as number of bits required to represent single color component of image. As compression ratio increases, number of bits per pixel are decreased (i.e. they are inversely proportional to each other). The visual representation of PSNR with respect to BPP (bits per pixel) of decryption without keys, with wrong keys and with all accurate keys is shown in Figure 5.10. It represents the variation in PSNR of video frames with the change in bits per pixel rate and keys used for decryption. If all keys are correct then will be high PSNR with high BPP, but if video is decrypted without keys or with wrong keys then PSNR is almost same in both cases. This

shows that the decryption with wrong keys will not affect the PSNR to large extent; it will be same as PSNR of encrypted frame. For better results optimized compression ratio should be chosen.

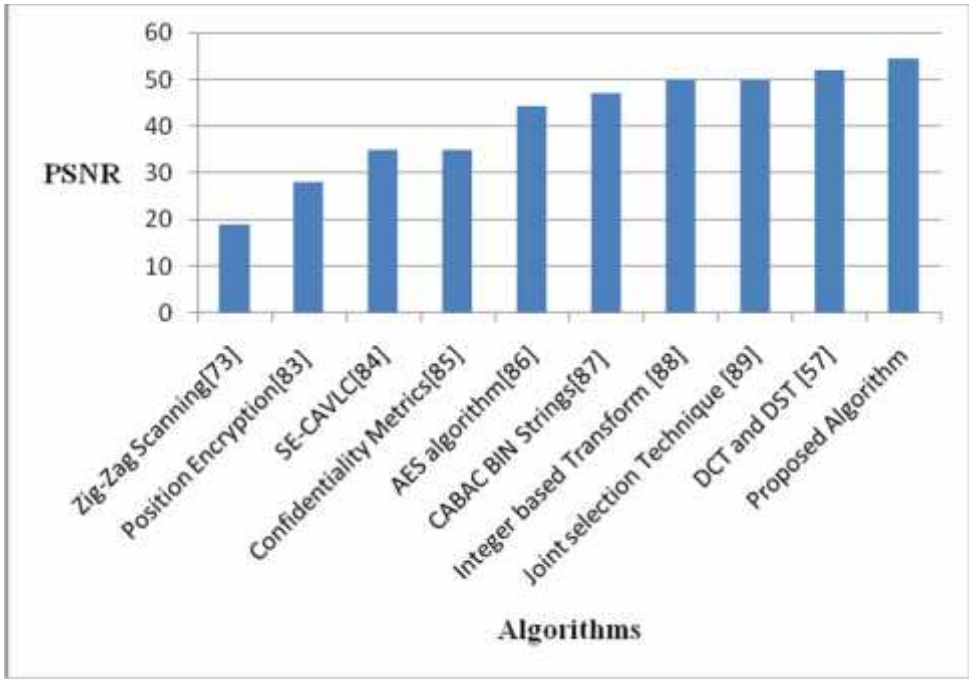


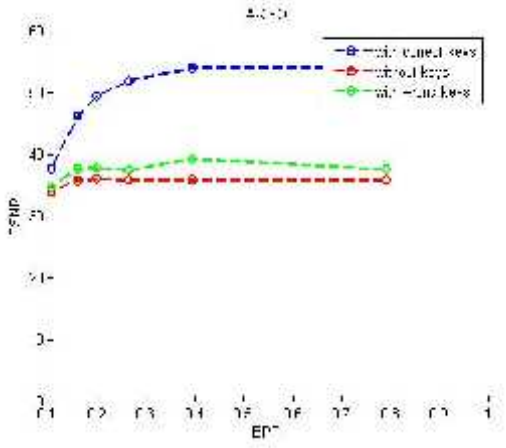
Figure 5.9 Bar graph representation of PSNR comparison with existing techniques

MSE is measured to ensure the presence of error in the decrypted video after reaches at the reception end. The average MSE of frames of test sequences is given in the Table 5.2.

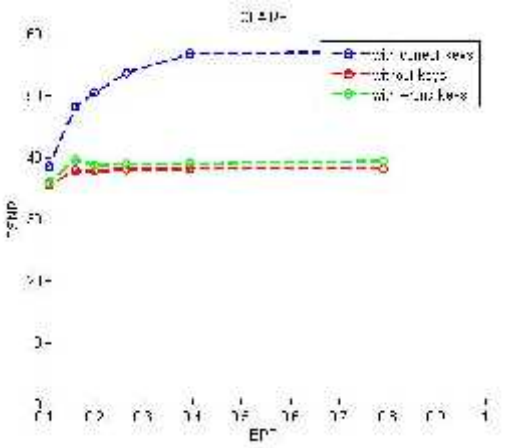
Compression Ratio	Video Sequences					
	Akiyo	Deadline	Lady	Grandma	Claire	Foreman
10%	0.3139	0.5560	0.3240	0.3544	0.2894	1.1439
20%	0.4152	0.6363	0.3366	0.4799	0.3028	1.3726
30%	0.5089	1.2147	0.3288	0.6362	0.3729	1.924
40%	0.7955	1.8862	0.4875	0.8687	0.6486	3.4089
50%	1.5908	4.3903	1.1986	1.7680	1.0216	6.179
75%	11.4197	22.4755	10.1602	8.3034	9.3316	33.29

Table 5.2 Average MSE of test videos

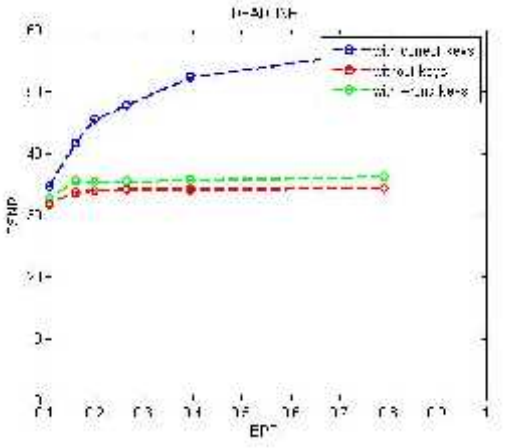
From the Table 5.2, it is concluded that as the CR is increased, the MSE is also increased, but requirement is having MSE as low as possible. Thus, there is dilemma between CR and MSE, the optimized value of CR should be chosen according to the requirement of application. The main requirement is minimum presence of error after the decryption must be minimum, so that original copy of the transmitted information can be received at the reception side. MSE is also considered as one of the quality parameter to determine the quality of encryption algorithm.



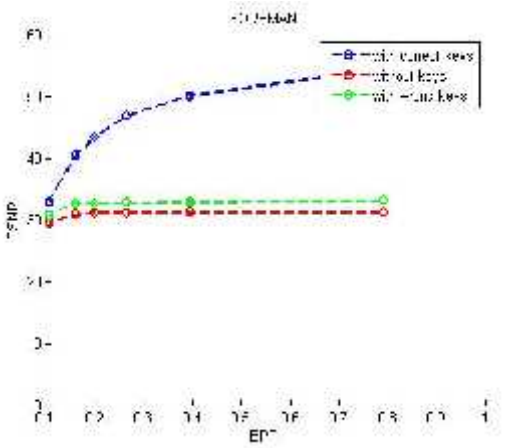
(a) Akiyo



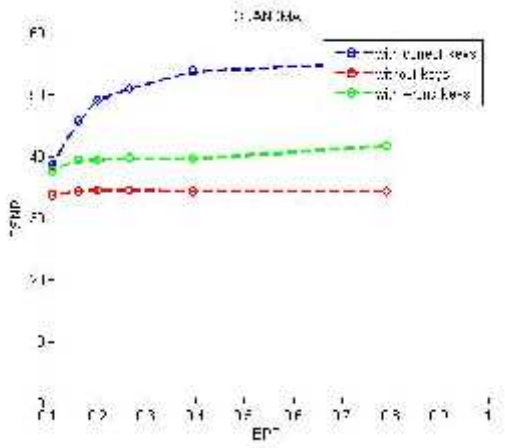
(b) Claire



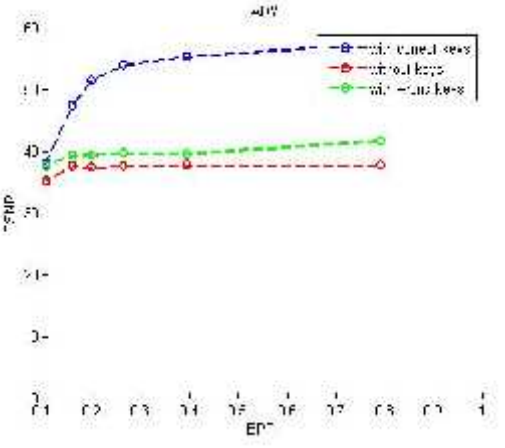
(c) Deadline



(d) Foreman

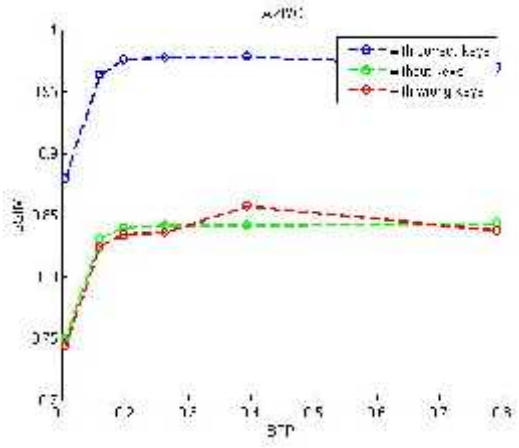


(e) Grandma

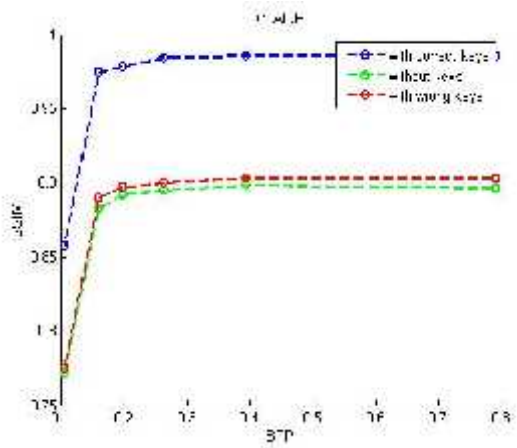


(f) Lady

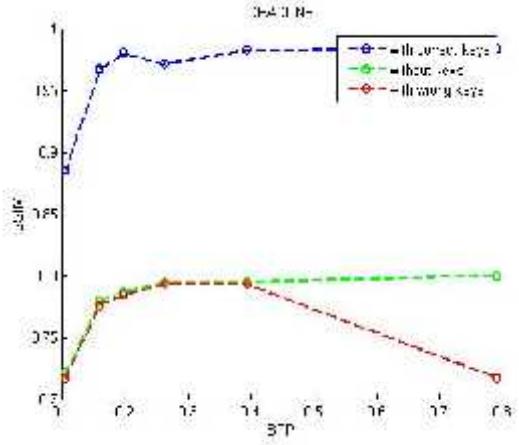
Figure 5.10 Visual representation of PSNR vs BPP for some test sequences



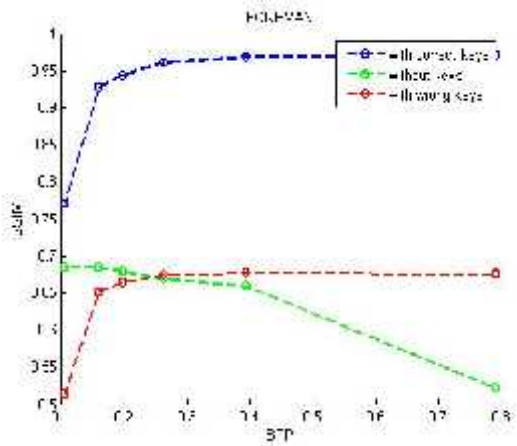
(a) Akiyo



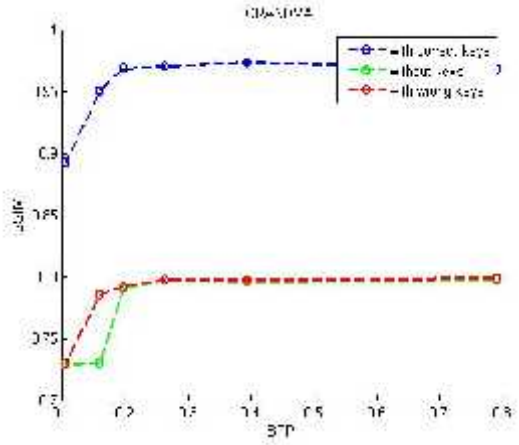
(b) Claire



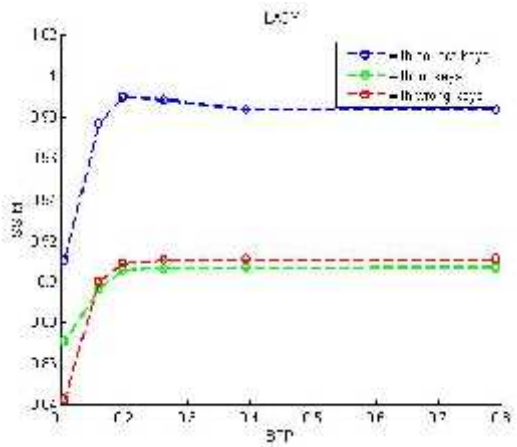
(c) Deadline



(d) Foreman



(e) Grandma



(f) Lady

Figure 5.11 Visual representation of SSIM vs BPP for some test sequences

SSIM is calculated to prove the similarity content in the original and decrypted video. The average SSIM with frames of video for some test sequences is shown in Figure 5.11.

Compression Ratio	Test Video Sequences					
	Akiyo	Deadline	Lady	Grandma	Claire	Foreman
10%	0.9687	0.9839	0.9840	0.9683	0.9840	0.9711
20%	0.9784	0.9827	0.9841	0.9736	0.9858	0.9686
30%	0.9780	0.9715	0.9889	0.9706	0.9844	0.9619
40%	0.9758	0.9799	0.9903	0.9687	0.9784	0.9439
50%	0.9634	0.9669	0.9772	0.9507	0.9747	0.9275
75%	0.8805	0.8857	0.9108	0.8926	0.8575	0.7705

Table 5.3 Average SSIM of test videos with proposed algorithm

The value of SSIM given in the Table 5.3 shows that as the compression ratio is increased, similarity of decrypted data is decreased. So, here optimized CR should be chosen for better results. The graph between SSIM and BPP in Figure 5.11 shows visual representation of similarity index of decrypted videos without keys, with wrong keys and with all correct keys. This represents maximum similarity of decrypted video with original video if all keys are correct and very low similarity index for videos decrypted without keys and with wrong keys. This will prevent attackers to draw relationship between encrypted video and decrypted video with hit and trail methods.

GMSD (Gradient Magnitude Similarity Deviation) is defined as the parameter that is used for the quality assessment. It is called as full reference parameter, which computes local quality map (LQM) between references or actual frame and distorted or decrypted frame and calculate final quality score using standard deviation. Initially, it calculates gradient magnitude of actual and decrypted frame, which is responsive to blurring, additive noise and compression etc. The pixel-wise similarity between actual and decrypted image is calculated for the LQM. For computing GMSD, initially calculate gradient magnitude similarity (GMS) [90] using:

$$GMS(j) = \frac{2m_a(j)m_d(j) + p}{m^2{}_a(j) + m^2{}_d(j) + p} \tag{5.1}$$

where, p is positive constant for numerical stability, m_a and m_d are gradient magnitudes of actual and decrypted frame given as:

$$m_a(j) = \sqrt{(\mathrm{a} \otimes v_x)^2(j) + (\mathrm{a} \otimes v_y)^2(j)} \tag{5.2}$$

$$m_d(j) = \sqrt{(\mathrm{d} \otimes v_x)^2(j) + (\mathrm{d} \otimes v_y)^2(j)} \tag{5.3}$$

where, v_x *and* v_y are Prewitt filters along x (horizontal direction) and y (vertical direction) is given as follows:

$$v_x = \begin{bmatrix} 1/3 & 0 & -1/3 \\ 1/3 & 0 & -1/3 \\ 1/3 & 0 & -1/3 \end{bmatrix} \tag{5.4}$$

$$v_y = \begin{bmatrix} 1/3 & 1/3 & 1/3 \\ 0 & 0 & 0 \\ -1/3 & -1/3 & -1/3 \end{bmatrix} \tag{5.5}$$

Now other parameter for calculating GMSD is gradient magnitude similarity mean (GMSM) which is calculated as follows:

$$GMSM = \frac{1}{M}\sum_{j=1}^{M} GMS(j) \tag{5.6}$$

Finally, for calculating GMSD formula is given as:

$$GMSD = \sqrt{\frac{1}{M}\sum_{j=1}^{M}(GMS(j) - GMSM)^2} \tag{5.7}$$

where, GMS and $GMSM$ are calculated from Equation (5.1) and equation (5.6) respectively. This parameter is calculated to check quality of retrieved videos at receiver side. If GMSD is low that means quality is higher. The average GMSD for the video frames is given in Table 5.4.

Compression Ratio	Test Video Sequences					
	Akiyo	Deadline	Lady	Grandma	Claire	Foreman
10%	0.0104	0.0546	2.7×10^{-6}	0.0703	0.0420	0.0166
20%	0.0104	0.0242	3.5×10^{-5}	0.0691	0.0420	0.0260
30%	0.0104	0.0546	1.03×10^{-4}	0.0680	0.0419	4.2×10^{-4}
40%	0.0489	0.0025	2.4×10^{-4}	0.0673	0.0430	0.0996
50%	0.0494	0.0667	7.5×10^{-4}	0.0017	0.0429	0.0953
75%	0.0233	0.0527	0.0167	0.0623	0.0512	0.0420

Table 5.4 GMSD of test videos with proposed algorithm

The value of GMSD as given in Table 5.4 shows that as the compression ratio is increasing, GMSD is decreasing. So, better compression ratio should be chosen to avoid blurring, additive noise etc. at decryption side.

The experimental results prove that proposed technique better results than existing techniques. The proposed algorithm also provides resistance from several attacks that are discussed in following section.

5.3.1 Analysis of Key Space

The analysis of key space is required to calculate space of key that is used for the encryption process. It should be as large as possible for good encryption technique. In proposed method, key is generated using biometrics for encryption of key. For calculating the space of key, two sequences are generated using $©$ and $© + w$ respectively $©$ and $\tilde{©}$, having length T_1. $© = \{0 < h(g) < 1 \mid 0 < g < L_1\}$ and $\tilde{©} = \{0 < \tilde{h}(g) < 1 \mid 0 < g < L_1\}$. The expression for mean absolute error is given as [42].

$$M(©, \tilde{©}) = \frac{1}{T_1} \sum_{g=1}^{T_1} \left| © (g) - \tilde{©} (g) \right| \tag{5.8}$$

The key space is given as $\frac{1}{w_0}$, w_0 is given as value of w where, M is zero. After the calculation the value of w_0 is 10^{-25}. So, key space for proposed algorithm is 10^{25}, which is huge to protect videos from brute force attacks.

5.4 ATTACKS

The proposed technique for the partial video encryption is robust; it protects video from several attacks that are applied by the intruder, for the data extraction from encrypted videos. The various attacks such as ciphertext only attack (COA), known plaintext attack (KPA), chosen ciphertext attack (CCA), brute force attack (BFA), man in middle attack (MIM) etc. are discussed in detail in proceeding section.

5.4.1 Cipher Only Attack (COA)

In the ciphertext only attack [91], the intruder doesn't have any idea about the key used for encryption. Attacker tries to calculate the key to hack information. The encrypted video in proposed algorithm is free from COA because of the use of biometric keys (iris and fingerprint), so attacker won't be able to calculate it, without the presence of original biometric. It is also called as replacement attacks.

5.4.2 Known Plaintext Attack (KPA)

In known plaintext attacks [91], the attacker has some plaintexts and their corresponding ciphertext also, with use of them unauthorized person tries to calculate the relation between original and encrypted information. In proposed algorithm iris and fingerprint two asymmetric keys are applied alternatively on each frame of video. So, even if the hacker gets

the information about public key, he won't be able to extract original information, without the presence of private key. In this way proposed algorithm is free from KPA attacks.

5.4.3 Chosen Ciphertext Attack (CCA)

In CCA [92], only ciphertext or encrypted data is used to hack the information, by doing little change in encrypted information and observing variation from frame to frame of video. Due to use of two different biometric keys (iris or fingerprint) for different frames, the observation between two ciphered frames will not facilitate hacker to deduce relation between them. So, the video is secured from chosen ciphertext attacks.

5.4.4 Brute Force Attack (BFA)

In BFA attack [91], the algorithm is known to the attackers, but key space is made large enough to protect key from them. The space of the key used for encryption is 10^{25}. So, even if he tries to get calculate key with hit and trail method it will not be easy for him to get correct key and it will take very large time to calculate the exact key. As, two keys are used for the better security so, hacker has to calculate two keys to get whole video.

5.4.5 Man In Middle Attack (MIM)

In MIM attacks **[**92**]** the attacker (E) is in the middle of sender (A) and receiver (B). When A tries to communicate with B, E as respond to the request of A. So, in this way the information send to the B will come through E. To protect the information from E, the video is encrypted using asymmetric key, that is generated by difference of biometrics of A and B. In which the biometric of receiver is also scanned at the reception side in order to decrypt the original information from the encrypted one. So, even if the intruder hack the data before it reaches at the reception side, no information will be leaked through it.

In this way due to use of duo biometric keys for the encryption of videos, the information is highly secure from the invaders.

5.5 SUMMARY

A multimodal biometric based partial encryption using DP-FrWT and scrambling is proposed to protect video information from the intruders. The comparison of PSNR of proposed technique with existing techniques proves that it provides better PSNR results with 3 dB more than existing techniques hence improved. Due to use of biometric keys, the videos encrypted with this technique are secured from cipher only attacks. The use of asymmetric

keys prevents videos from known plaintext attacks also, the large key space of 10^{25} resists from brute force attacks. In this way proposed algorithm, provides better results as well protection from several attacks.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 CONCLUSION

This thesis represents performance analysis of fractional transforms for the application encryption and compression. The improvement in the algorithms with the use of fractional transform in combination with scrambling and multimodal biometric keys provides better performance. The security analysis of image and video encryption proves the better results of proposed techniques in comparison with existing methods. The proposed algorithm also resists the attacks on the encrypted information while travelling through the open channel.

The images are secured using encryption technique consisting of DP-FrWT, scrambling and biometric keys. The keys used for the encryption of images are symmetric biometric keys (i.e. Iris and Fingerprint). The simulation results of image encryption provides infinite PSNR, zero MSE thus approximately generate exact copy of original image at the reception side. The correlation coefficients as well as histogram analysis shows the randomization in the encrypted information, that prevents images from histogram attacks. The observation of entropy provides idea about the probability of prediction of information from the ciphered data. The implementation of differential attacks and spoofing attacks provide security from the several attacks applied during the transmission of information through the unsafe network.

The video encryption is performed using region of interest based encryption, in which portion of frame is selected and encrypted. Before encryption of videos DFrFT is used to compress the videos, to save the bandwidth requirement for the transmission of the video information. The simulation results of the video encryption provide 3dB above PSNR than the existing techniques. The keys space analysis provides resistance of algorithm from the brute force attacks with the key space of 10^{25}, which is large enough to be guessed. It also defends against several attacks like CPA, KPA, MIM, CCA etc. due to use of asymmetric biometric keys for the encryption of videos.

Thus, it is summarized that the use of DP-FrWT provides far better results than the existing algorithms by using in combination with scrambling and biometric keys for the encryption of multimedia contents such as images and videos. The DFrFT is considered better for the

compression of videos among the fractional transforms to save the bandwidth and storage space for the transmission and storing of information respectively.

6.2 FUTURE SCOPE

The development in the existing algorithms is a continuous process, as one of the algorithm has taken into account for the encryption of information. The use of biometrics provides highly confidential keys for the encryption process, because they don't require space for storing. So, use of biometric keys improves the performance of existing fractional transform, so even more complicated transform can be introduced to prevent intervention of invaders. The security of information is getting very important task due to digitalization of world in almost every area, but another important aspect is reduction in computational time while the encryption of information.

REFERENCES

[1] Tamilarasi R, Prabu S and Swarnalatha P, "An Approach for Data and Image Security in Public Cloud using Segmentation and Authentication (CSA) Protocol Suite." MAGNT Research Report 2015. 133-141.

[2] Saxena R and Singh K (2013). Fractional Fourier transform: A novel tool for signal processing, *Journal of the Indian Institute of Science*, 85(1), 11.

[3] Singh K and Saxena RG. Performance of discrete fractional Fourier transform classes in signal processing applications. Ph.D. Thesis, Thapar University, Patiala, India, 2006.

[4] Wiener N (1929). Hermitian polynomials and Fourier analysis, *Studies in Applied Mathematics*, 8(1-4), 70-73.

[5] Zhang L, Wu J and Zhou N (2009). Image encryption with discrete fractional cosine transform and chaos, *International Conference on Information Assurance and Security* [5th: 2009], 2, pp. 61-64.

[6] Singh H (2016). Cryptosystem for Securing Image Encryption Using Structured Phase Masks in Fresnel Wavelet Transform Domain, *3D Research*, 7(4), 34.

[7] Bhatnagar G and Wu QJ (2014). Biometric inspired multimedia encryption based on dual parameter fractional Fourier transform, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(9), 1234-1247.

[8] Li X and Zhao D (2010). Optical color image encryption with redefined fractional Hartley transform, *Optik-International Journal for Light and Electron Optics*, 121(7), 673-677.

[9] Zhou N, Wang Y and Gong L (2011). Novel optical image encryption scheme based on fractional Mellin transform, *Optics Communications*, 284(13), 3234-3242.

[10] Baby D *et al.* (2015). A novel DWT based image securing method using steganography, *Procedia Computer Science*, 46, 612-618.

[11] Lai CC and Tsai CC (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition, *IEEE Transactions on instrumentation and measurement*, 59(11), 3060-3063.

[12] Li S and Zheng X (2002). Cryptanalysis of a chaotic image encryption method, *IEEE International Symposium on Circuits and Systems*, 2.

[13] Fridrich J and Binghamton S (1997). Image encryption based on chaotic maps, *IEEE International Conference on Systems, Man, and Cybernetic Computational Cybernetics and Simulation* [USA: 1997], 2, pp. 1105-1110.

[14] Bibhudendra A, Patra SK and Panda G (2008). Image encryption by novel cryptosystem using matrix transformation, *First International Conference on Emerging Trends in Engineering and Technology*, pp. 77-81.

[15] Sun Q *et al.* (2012). A novel digital image encryption method based on one-dimensional random scrambling, *International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)* [9th : 2012], pp. 1669-1672.

[16] Cheng H and Li X (2000). Partial encryption of compressed images and videos, *IEEE Transactions on signal processing*, 48(8), 2439-2451.

[17] Xu S *et al.* (2008). Cryptanalysis of two chaotic image encryption schemes based on permutation and XOR operations, *International Conference on Computational Intelligence and Security*, 2, pp. 433-437.

[18] Tang Z, Zhang X and Lan W (2015). Efficient image encryption with block shuffling and chaotic map, *Multimedia tools and applications*, 74(15), 5429-5448.

[19] Choudhary NY and Gupta RK (2014). Partial Image Encryption based on Block wise Shuffling using Arnold Map, *International Journal of Computer Applications*, 97(10).

[20] Hazarika N and Saikia M (2014). A novel partial image encryption using chaotic logistic map, *International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 231-236.

[21] Chaudhary MK and Pandi MG (2015). A Survey on Secured Real Time Video Transmission with Significant Improvement in Privacy Preservation, *International Journal of Engineering Development and Research*, 3, 205-211.

[22] Abuturab MR (2015). An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform, *Optics and Lasers in Engineering*, 69, 49-57.

[23] Luo Y, Du M and Liu J (2015). A symmetrical image encryption scheme in wavelet and time domain, *Communications in Nonlinear Science and Numerical Simulation*, 20(2), 447-460.

[24] Yaschenko, VV. Cryptography: An Introduction. Available at http://bookstore.ams.org/stml-18 (Accessed on 9th May 2017).

[25] Washington DC. U.S. History: Our Worst Subject? Available at https://global.oup.com/academic/content/series/h/a-history-of-us-hus/?cc=in&lang=en& (Accessed on 9th May 2017).

[26] Diffie W and Hellman M (1976). New directions in cryptography, *IEEE transactions on Information Theory*, 22(6), 644-654.

[27] Bultheel A and Martinez S H, "A shattered survey of the Fractional Fourier Transform," 2002.

[28] Sansone G. *Orthogonal functions*. Courier Corporation, 1959.

[29] Jindal N and Singh K. Performance of Fractional Transforms in Image and Video Processing. Ph.D. Thesis, Thapar University, Patiala, India, 2013.

[30] Mendlovic D *et al.* (1997). Fractional wavelet transform, *Applied optics*, 36(20), 4801-4806.

[31] Zhu B, Liu S and Ran Q (2000). Optical image encryption based on multifractional Fourier transforms, *Optics letters*, 25(16), 1159-1161.

[32] Hennelly BM and Sheridan JT (2003). Optical image encryption by random shifting in fractional Fourier domains, *Optics Letters*, 28(4), 269-271.

[33] Hennelly BM and Sheridan JT (2005). Generalizing, optimizing, and inventing numerical algorithms for the fractional Fourier, Fresnel, and linear canonical transforms, *JOSA A*, 22(5), 917-927.

[34] Refregier P and Javidi B (1995). Optical image encryption based on input plane and Fourier plane random encoding, *Optics Letters*, 20(7), 767-769.

[35] Unnikrishnan G and Singh K (2000). Double random fractional Fourier-domain encoding for optical security, *Optical Engineering*, 39(11), 2853-2859.

[36] Liu S, Yu L and Zhu B (2001). Optical image encryption by cascaded fractional Fourier transforms with random phase filtering, *Optics Communications*, 187(1), 57-63.

[37] Li S *et al.* (2008). Cryptanalysis of an image scrambling scheme without bandwidth expansion, *IEEE Transactions on Circuits and Systems for Video Technology*, 18(3), 338-349.

[38] Zayed AI (1998). A convolution and product theorem for the fractional Fourier transform, *IEEE Signal processing letters*, 5(4), 101-103.

[39] Luo X, Fan J and Wu J (2012). March. Single-channel color image encryption based on the Multiple-order discrete fractional Fourier transform and chaotic scrambling. *International Conference on Information Science and Technology (ICIST)*, pp. 780-784.

[40] Zou J and Ward RK (2003). Introducing two new image scrambling methods, *Pacific Rim Conference on Communications, Computers and signal Processing, PACRIM*, 2, pp. 708-711.

[41] Zou J, Ward RK and Qi D (2004). A new digital image scrambling method based on Fibonacci numbers, *International Symposium on Circuits and Systems, ISCAS'04*, 3, pp. III-965.

[42] Zhang HY (2007). A new image scrambling algorithm based on queue transformation, *International Conference on Machine Learning and Cybernetics*, 3, pp. 1526-1530.

[43] Zhang HY (2008). A new image scrambling algorithm, *International Conference on Machine Learning and Cybernetics*, 2, pp. 1088-1092.

[44] Liping S *et al*. (2008). Image scrambling algorithm based on random shuffling strategy, *International Conference on Industrial Electronics and Applications, ICIEA* [3rd: 2008], pp. 2278-2283.

[45] Agi I and Gong L (1996). An empirical study of secure MPEG video transmissions. *Proceedings of the Symposium on Network and Distributed System Securit*, pp. 137-144.

[46] Spanos GA and Maples TB (1995). Performance study of a selective encryption scheme for the security of networked, real-time video. *International Conference on Computer Communications and Networks*, [4th: 1995], pp. 2-10.

[47] Liu F and Koenig H (2010). A survey of video encryption algorithms, C*omputers & Security*, 29(1), 3-15.

[48] Jindal N and Singh K (2014). Image and video processing using discrete fractional transforms. *Signal, Image and Video Processing*, 8(8), 1543-1553.

[49] Meyer J and Gadegast F. Security mechanisms for multimedia data with the example MPEG-I video, 1995.

[50] Agi I and Gong L (1996). An empirical study of secure MPEG video transmissions, *In Proceedings of the Symposium on Network and Distributed System Security*, pp. 137-144.

[51] Liu F and Koenig H (2010). A survey of video encryption algorithms, *Computers & Security*, 29(1), 3-15.

[52] Spanos GA and Maples TB (1996). Security for real-time MPEG compressed video in distributed multimedia applications, *International Phoenix Conference on Computers and Communications* [5th: 1996], pp. 72-78.

[53] Qiao L and Nahrstedt K (1998). Comparison of MPEG encryption algorithms, *Computers & Graphics*, 22(4), 437-448.

[54] Shi C and Bhargava B (1998). A fast MPEG video encryption algorithm. *In Proceedings of the sixth ACM international conference on Multimedia*, pp. 81-88.

[55] Shi C, Wang SY and Bhargava B (1999). MPEG video encryption in real-time using secret key cryptography. *In Proceedings Int. Conf. Parallel and Distributed Processing Techniques and Applications*.

[56] Yeung SKA, Zhu S and Zeng B (2011). Design of new unitary transforms for perceptual video encryption, *IEEE Transactions on Circuits and Systems for Video Technology*, 21(9), 1341-1345.

[57] Yeung SKA and Zeng B (2012). A new design of multiple transforms for perceptual video encryption. *International Conference on Image Processing (ICIP)* [19th: IEEE, 2012], pp. 2637-2640.

[58] Peng F, Zhu XW and Long M (2013). An ROI privacy protection scheme for H. 264 video based on FMO and Chaos, *IEEE transactions on information forensics and security*, 8(10), 1688-1699.

[59] Rajagopal S and Shenbagavalli M (2013). Partial Video Encryption Using Random Permutation Based on Modification on DCT Based Transformation, *IRJES*, 2(6), 54-58.

[60] Wang Y, O'Neill M and Kurugollu F (2013). Partial encryption by randomized zig-zag scanning for video encoding, *International Symposium on Circuits and Systems (ISCAS)*, pp. 229-232.

[61] Towards a Replacement for the DVB Common Scrambling Algorithm, Farncombe Consulting Group, UK, 2009.

[62] Zeng W and Lei S (2003). Efficient frequency domain selective scrambling of digital video, *IEEE Transactions on Multimedia*, 5(1), 118-129.

[63] Tang L (1997). Methods for encrypting and decrypting MPEG video data efficiently, *In Proceedings of the fourth ACM international conference on Multimedia*, pp. 219-229.

[64] Wang Y, Cai M and Tang F (2007). Design of a new selective video encryption scheme based on H. 264, *International Conference on Computational Intelligence and Security*, pp. 883-882.

[65] Monrose F *et al.* (2001). Cryptographic key generation from voice, *IEEE Symposium on Security and Privacy*, pp. 202-213.

[66] Zhang W and Chen T (2005). Generalized optimal thresholding for biometric key generation using face images, *International Conference on Image Processing, ICIP*, 3, pp. III-784.

[67] Daugman J (2004). How iris recognition works, *IEEE Transactions on circuits and systems for video technology*, 14(1), 21-30.

[68] Nguyen THL and Nguyen TTH (2008). An approach to protect private key using fingerprint biometric encryption key in BioPKI based security system, *International Conference on Control, Automation, Robotics and Vision, ICARCV* [10th: 2008], pp. 1595-1599.

[69] Hoque S, Fairhurst M and Howells G (2008). Evaluating biometric encryption key generation using handwritten signatures, *ECSIS Symposium on Bio-inspired Learning and Intelligent Systems for Security, BLISS'08*, pp. 17-22.

[70] Wu X, Wang K and Zhang D (2008). A cryptosystem based on palmprint feature, *International Conference on Pattern Recognition, ICPR* [19th: 2008], pp. 1-4.

[71] Chen CK and Lin CL (2010). Text encryption using ECG signals with chaotic Logistic map, *IEEE Conference on Industrial Electronics and Applications (ICIEA)*, [5th: 2010], pp. 1741-1746.

[72] China unveils world's first facial recognition ATM. Available at http://www.telegraph.co.uk/news/worldnews/asia/china/11643314/China-unveils-worlds-first-facial-recognition-ATM.html

[73] Bhatnagar G, Wu QJ and Raman B (2013). Discrete fractional wavelet transform and its application to multiple encryption, *Information Sciences*, 223, 297-316.

[74] Ozaktas HM and Kutay MA (2001). The fractional Fourier transform, *European Control Conference (ECC)*, pp. 1477-1483.

[75] Shi J, Zhang N and Liu X (2012). A novel fractional wavelet transform and its applications, *Science China Information Sciences*, 55(6), 1270-1279.

[76] Wu J, Guo F and Zhou N (2013). Single-Channel Color Image Encryption Using the Reality-Preserving Fractional Discrete Cosine Transform in YCbCr Space, *JCP*, 8(11), 2816-2822.

[77] Naik K and Pal AK (2015). Design of a cryptosystem for DCT compressed image using Arnold transform and fractional Fourier transform, *International Journal of Computational Vision and Robotics*, 5(3), 335-346.

[78] Sinha A and Singh K (2013). Image encryption using fractional Fourier transform and 3D Jigsaw transform, *Optical Engineering*.

[79] Sui L, Duan K and Liang J (2015). Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps, *Optics Communications*, 343, 140-149.

[80] Lima JB and Novaes LFG (2014). Image encryption based on the fractional Fourier transform over finite fields, *Signal Processing*, 94, 521-530.

[81] Xu L *et al.* (2016). A novel bit-level image encryption algorithm based on chaotic maps, *Optics and Lasers in Engineering*, 78, 17-25.

[82] Pan SM *et al.* (2017). Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform, *Multimedia Tools and Applications*, 76(2), 2933-2953.

[83] Wang Q and Wang, X (2014). A new selective video encryption algorithm for the H. 264 standard, *International Conference on Progress in Informatics and Computing (PIC)*, pp. 275-279.

[84] Dubois L, Puech W and Blanc-Talon J (2011). Fast protection of H. 264/AVC by reduced selective encryption of CAVLC, *European Signal Processing Conference* [19th: IEEE, 2011], pp. 2185-2189.

[85] Dubois L, Puech W and Blanc-Talon J (2014). Smart selective encryption of H. 264/AVC videos using confidentiality metrics, *Annals of Telecommunications-annales des télécommunications*, 69(11-12), 569-583.

[86] Shahid Z, Chaumont M and Puech W (2011). Fast protection of H. 264/AVC by selective encryption of CAVLC and CABAC for I and P frames, *IEEE Transactions on Circuits and Systems for Video Technology*, 21(5), 565-576.

[87] Asghar M, *et al.* (2012). Efficient selective encryption with H. 264/SVC CABAC bin-strings. *International Conference on Image Processing (ICIP)* [19th: IEEE, 2012], pp. 2645-2648.

[88] Zeng B *et al.* (2014). Perceptual encryption of H. 264 videos: Embedding sign-flips into the integer-based transforms, *IEEE transactions on information forensics and security*, 9(2), 309-320.

[89] Tew Y, Wong K and Phan RCW (2016). Joint selective encryption and data embedding technique in HEVC video, *Annual Summit and Conference Signal and Information Processing Association (APSIPA)* [Asia-Pacific, 2016], pp. 1-5.

[90] Xue W *et al.* (2014). Gradient magnitude similarity deviation: A highly efficient perceptual image quality index, *IEEE Transactions on Image Processing*, 23(2), 684-695.

[91] Li S *et al.* (2008). Cryptanalysis of an image scrambling scheme without bandwidth expansion, *IEEE Transactions on Circuits and Systems for Video Technology*, 18(3), 338-349.

[92] Wang J *et al.* (2007). A partial scramble scheme for H. 264 video, *International Conference on ASIC* [7th: 2007], pp. 802-805.

LIST OF PUBLICATIONS

[1] Kaur J. *et al.* (2017). Image Encryption using Fractional Transforms and Biometric keys - A Review, *International Conference on Advancements in Engineering and Technology* [5th : Punjab, India: 24 March 2017], pp. 46-50.

[2] Kaur J *et al.* (2017). Video Security using fractional transforms and scrambling in combination with multimodal biometric keys, *International Journal of Computer Science and Information Security-Scopus Indexed (Online published),* 15(6), 309-323.

[3] Kaur J *et al.* (2017). A Secure Image Encryption Algorithm based on Fractional Transform and Scrambling with Multimodal Biometric keys, *Sadhana-Springer, Communicated. (SCI Indexed).*

Turnitin Originality Report

801561010 by Jobanpreet Kaur

From 123 (paper1)

Processed on 12-Jul-2017 13:03 IST
ID: 830400638
Word Count: 21745

Similarity Index	Similarity by Source	
8%	Internet Sources:	4%
	Publications:	6%
	Student Papers:	3%

sources:

1 < 1% match (student papers from 22-Jul-2016)
Submitted to Higher Education Commission Pakistan on 2016-07-22

2 < 1% match (publications)
Krishnamoorthy, R., and P. Murali. "Symmetric image encryption scheme based on multiple chaotic maps", 2012 International Conference on Emerging Trends in Science Engineering and Technology (INCOSET), 2012.

3 < 1% match (student papers from 07-Jul-2015)
Submitted to Thapar University, Patiala on 2015-07-07

4 < 1% match (publications)
Bhatnagar, Gaurav, and Q. M. Jonathan Wu. "Biometric Inspired Multimedia Encryption Based on Dual Parameter Fractional Fourier Transform", IEEE Transactions on Systems Man and Cybernetics Systems, 2014.

5 < 1% match (student papers from 11-Jul-2017)
Submitted to Thapar University, Patiala on 2017-07-11

6 < 1% match (student papers from 12-Feb-2016)
Submitted to Arts, Sciences & Technology University In Lebanon on 2016-02-12

7 < 1% match (Internet from 16-May-2016)
http://archive.org/stream/theapp00cozz/theapp00cozz_djvu.txt

8 < 1% match (student papers from 06-Jul-2015)
Submitted to Thapar University, Patiala on 2015-07-06

9 < 1% match (student papers from 21-Jun-2015)
Submitted to Thapar University, Patiala on 2015-06-21

10 < 1% match (student papers from 06-Jun-2014)
Submitted to Thapar University, Patiala on 2014-06-06

11 < 1% match (publications)
Jindal, N., and K. Singh. "Joint image compression–encryption using discrete fractional transforms", The Imaging Science Journal, 2014.

12 < 1% match (publications)
Smit Trambadia, Hemant Mayatra. "Gradient-Kalman Filtering (GKF) based endoscopic image restoration", 2015 5th Nirma University International Conference on Engineering (NUiCONE), 2015

13 < 1% match (publications)
Fernandes, Steven Lawrence, and G. Josemin Bala. "Developing a Novel Technique to Match Composite Sketches with Images Captured by Unmanned Aerial Vehicle", Procedia Computer Science, 2016.

14 < 1% match ()
http://lrd.yahooapis.com/_ylc=X3oDMTVnZnZodWJlBF9TAzIwMjMxNTI3MDIEYXBwaWQDTHJlazRUTFYzNEdRVjYwVDFRYVlHeC5xMDYu

15 < 1% match (publications)
Wavelet Transforms and Their Applications, 2015.

16 < 1% match (Internet from 12-Jun-2017)
http://www.i-scholar.in/index.php/indjst/article/view/128334/116707

17 < 1% match (publications)
SIVAKUMAR, T. and VENKATESAN, R.. "A New Image Encryption Method Based on Knight's Travel Path and True Random Number", Journal of Information Science & Engineering, 2016.

18 < 1% match (publications)
Du, Zheng-Cong, De-Ping Xu, and Jin-Ming Zhang. "Fractional S-transform-part 2: Application to reservoir prediction and fluid identification", Applied Geophysics, 2016.

19 < 1% match (publications)
Elgendy, Fatma, Amany M. Sarhan, Tarek E. Eltobely, S. F. El-Zoghdy, Hala S. El-sayed, and Osama S. Faragallah. "Chaos-based model for encryption and decryption of digital images", Multimedia Tools and Applications, 2015.

20 < 1% match (publications)
Yaru, Liang, and Wu Jianhua. "New image encryption combining fractional DCT via polynomial interpolation with dependent scrambling and diffusion", The Journal of China Universities of Posts and Telecommunications, 2015.

21 < 1% match (Internet from 20-May-2014)
http://meteo.edu.vn/DATA/Dat_ECE/YeuTo/BH/BH_N1.dat

22 < 1% match (Internet from 11-Jun-2017)
http://documents.mx/documents/comparison-of-variants-of-blast.html

23 < 1% match (publications)
Gaurav Bhatnagar. "Encryption Based Robust Watermarking in Fractional Wavelet Domain", Studies in Computational Intelligence, 2009

24 < 1% match (student papers from 26-May-2011)
Submitted to University of Northumbria at Newcastle on 2011-05-26

25 < 1% match (publications)
Yakov Berkovich, Zvonimir Janko. "§95 Nonabelian 2-groups of exponent 2e which have no minimal nonabelian subgroups of exponent 2e", Walter de Gruyter GmbH, 2011

26 < 1% match (publications)
C. Narsimha Raju. "A real-time video encryption exploiting the distribution of the DCT coefficients", TENCON 2008 - 2008 IEEE Region 10 Conference, 11/2008

27 < 1% match (publications)
Communications in Computer and Information Science, 2015.

28 < 1% match (publications)
Studies in Computational Intelligence, 2016.

29 < 1% match (student papers from 23-Jun-2017)
Submitted to Nanjing Foreign Language School on 2017-06-23

30 < 1% match (student papers from 09-May-2012)
Submitted to Queen Mary and Westfield College on 2012-05-09

31 < 1% match (publications)
Sbiaa, Fatma Zayen, Medien Zeghid, Sonia Kotel, Rached Tourki, Mohsen Machhout, and Adel Baganne. "A Chaos-Based Approach for Correcting the Security Level of a Block Cipher Algorithm", International Review on Computers and Software (IRECOS), 2016.

32 < 1% match (Internet from 20-Dec-2014)
http://ijcsn.org/IJCSN-2014/3-6/Review-on-Various-Methods-for-Secure-Transmission-of-Images-for-Maintaining-Image-Integrity.pdf

33 < 1% match (publications)
Jiang, Yicheng, and Yun Zhang. "Motion estimation and focusing of ships in TerraSAR-X data using FrFT", 2012 IEEE International Geoscience and Remote Sensing Symposium, 2012.

34 < 1% match (publications)
Marcin Dudziński. "The almost sure central limit theorems for certain order statistics of some stationary Gaussian sequences", Annales UMCS Mathematica, 01/01/2009

35 < 1% match (publications)
Yi, Jiawang, and Guanzheng Tan. "Halving the dimension of a single image to be encrypted optically to avoid data expansion", Optical Engineering, 2016.

36 < 1% match (Internet from 31-Jan-2016)
http://doras.dcu.ie/18142/1/Eugene_O'Reilly.pdf

37 < 1% match (Internet from 11-Jun-2017)
http://eprints.ums.ac.id/26424/1/HALAMAN_DEPAN.pdf

38 < 1% match (Internet from 10-Oct-2015)
http://www.researchgate.net/profile/Agus_Harjoko/publication/274084777_Penyembunyian_Data_pada_File_Video_Menggunakan_Metode_

39 < 1% match (Internet from 06-May-2016)
http://airccj.org/CSCP/vol5/csit53602.pdf

40 < 1% match (publications)
Ping, Ping, Feng Xu, and Zhi-Jian Wang. "Image encryption based on non-affine and balanced cellular automata", Signal Processing, 2014.

41 < 1% match (student papers from 29-Mar-2015)
Submitted to October University for Modern Sciences and Arts (MSA) on 2015-03-29

42 < 1% match (Internet from 23-Jun-2017)
http://repository.um.edu.my/623/1/Enhancing%20Selective%20Encryption.pdf

43 < 1% match (Internet from 01-Jul-2017)
http://polen.itu.edu.tr/bitstream/11527/1129/1/9818.pdf

44 < 1% match (Internet from 01-Nov-2015)
http://worldwidescience.org/topicpages/i/imaging+system+parameters.html

45 < 1% match (publications)
Nidhi S. Kulkarni. "Multimedia Encryption: A Brief Overview", Studies in Computational Intelligence, 2009

46 < 1% match (student papers from 26-Nov-2012)
Submitted to University of Northumbria at Newcastle on 2012-11-26

47 < 1% match (Internet from 06-Mar-2012)
http://www.waset.org/journals/ijice/v2/v2-8-72.pdf

48 < 1% match (Internet from 02-Sep-2016)
http://www.apple.com/uk/ipad/compare/

49 < 1% match (publications)
Soo-Chang Pei. "The discrete fractional cosine and sine transforms", IEEE Transactions on Signal Processing, 6/2001

50 < 1% match (publications)
Pei, S.C.. "Two dimensional discrete fractional Fourier transform", Signal Processing, 19980529

51 < 1% match (publications)
Krishna, B. T.. "Fractional Fourier transform : a survey", Proceedings of the International Conference on Advances in Computing Communications and Informatics - ICACCI 12 ICACCI 12, 2012.

52 < 1% match (publications)
Mohindru, Pooja, Rajesh Khanna, and S. S. Bhatia. "An Improved Product Theorem for Fractional Fourier Transform", Proceedings of the National Academy of Sciences India Section A Physical Sciences, 2012.

53 < 1% match (Internet from 22-Dec-2012)
http://dspace.thapar.edu:8080/dspace/bitstream/10266/1782/1/PDFFile_Thesis_Khushboo.pdf

54 < 1% match (Internet from 07-Jun-2017)
http://www.iiisci.org/Journal/CV$/sci/pdfs/SA329GB14.pdf

55 < 1% match (Internet from 26-Feb-2012)
http://www.amostech.com/TechnicalPapers/2009/Poster/Dente.pdf

56 < 1% match ()
http://www.cse.unl.edu/~reich/csce472/Joint.pdf

57 < 1% match (Internet from 08-Jul-2003)
http://hbar.wustl.edu/~qwang/publications/qwang006.pdf

58 < 1% match (Internet from 23-Dec-2015)
http://ojs.academypublisher.com/index.php/jcp/article/download/jcp0902412419/8679

59 < 1% match (Internet from 10-Jul-2014)
http://www.statru.org/wp-content/uploads/2012/04/01_Statistical-Methods-in-Bioinformatics.pdf

60 < 1% match (publications)
Chenggi Wang, Xiao Zhang, Zhiming Zheng, "An efficient image encryption algorithm based on a novel chaotic map", Multimedia Tools and Applications, 2016

61 < 1% match (publications)
Liu, Ye, Jun Wang, Jinghui Fan, and Lihua Gong. "Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences", Multimedia Tools and Applications, 2015.

62 < 1% match (publications)
Ahmad, Jawad, Seong Oun Hwang, and Arshad Ali. "An Experimental Comparison of Chaotic and Non-chaotic Image Encryption Schemes", Wireless Personal Communications, 2015.

63 < 1% match (publications)
Zhou, Q., "On the security of multiple Huffman table based encryption", Journal of Visual Communication and Image Representation, 201101

64 < 1% match (publications)
SONTAKKE, P. K. and GUDADHE, A. S., "Convolution and Rayleigh's theorem for generalized fractional Hartley transform", xxx, 2009.

65 < 1% match (publications)
Deng, Juan, Shu Zhao, Yan Wang, Lei Wang, Hong Wang, and Hong Sha. "Image compression-encryption scheme combining 2D compressive sensing with discrete fractional random transform", Multimedia Tools and Applications, 2016.

66 < 1% match (publications)
Hukum Singh, "Cryptosystem for Securing Image Encryption Using Structured Phase Masks in Fresnel Wavelet Transform Domain", 3D Research, 2016

67 < 1% match (publications)
Vijay Kumar, Dinesh Kumar, "A modified DWT-based image steganography technique", Multimedia Tools and Applications, 2017

68 < 1% match (Internet from 22-Dec-2012)
http://dspace.thapar.edu:8080/dspace/bitstream/10266/1968/1/THESIS.pdf

69 < 1% match (Internet from 05-Jan-2015)
http://www.ijsett.com/images/Paper19(3).pdf

70 < 1% match (Internet from 24-Jun-2017)
http://ijceronline.com/papers/3-10.pdf

71 < 1% match (Internet from 11-Jul-2015)
http://web.mat.bham.ac.uk/C.W.Parker/Sarahs%20MPhil.pdf

72 < 1% match (Internet from 16-Dec-2015)
http://eprints.aston.ac.uk/20914/1/Studentthesis-2013.pdf

73 < 1% match (Internet from 11-Jul-2016)
https://www.deepdyve.com/browse/journals/ieee-transactions-on-systems-man-and-cybernetics-systems/2014/v44/i9?page=2

74 < 1% match (Internet from 29-Oct-2010)
http://www.cse.fau.edu/~borko/Chapter%203,%20MM%20Security.pdf

75 < 1% match (Internet from 09-Aug-2013)
http://ijpttjournal.org/volume-3/issue-1/IJPTT-V3I1P408.pdf

76 < 1% match (Internet from 15-May-2014)
http://researchbank.rmit.edu.au/eserv/rmit:160112/Shamshurin.pdf

77 < 1% match (Internet from 04-Dec-2010)
http://www.ecrypt.eu.org/ecrypt1/documents/D.WVL.5-1.0.pdf

78 < 1% match (Internet from 10-Nov-2013)
http://czytanki.net/channels/journal-computers

79 < 1% match (Internet from 03-Dec-2015)
http://www.uow.edu.au/~jennie/WEBPDF/1994_16.pdf

80 < 1% match (Internet from 20-Dec-2016)
https://ediss.uni-goettingen.de/bitstream/handle/11858/00-1735-0000-000D-F073-9/abramov.pdf?sequence=1

81 < 1% match (publications)
Murugan, Brindha, and Ammasai Gounden N. "An image encryption scheme based on block based confusion and multiple levels of diffusion", IET Computer Vision, 2016.

82 < 1% match (publications)
Rhouma Rhouma. "A new color image cryptosystem based on a piecewise linear chaotic map", 2009 6th International Multi-Conference on Systems Signals and Devices, 03/2009

83 < 1% match (publications)
Lecture Notes in Electrical Engineering, 2013.

84 < 1% match (publications)
Soni, A., J. Jain, and R. Roshan. "Image steganography using discrete fractional Fourier transform", 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), 2013.

85 < 1% match (publications)
Awwad , Aiman Mamdouh Ahmad Ayyal. "Digital Image Scrambling Method Based on Two Dimensional Cellular Automata : A Test of the Lambda Value", University of Jordan, 2009.

86 < 1% match (publications)
Liang, Yaru, Guoping Liu, Nanrun Zhou, and Jianhua Wu. "Image encryption combining multiple generating sequences controlled fractional DCT with dependent scrambling and diffusion", Journal of Modern Optics, 2014.

< 1% match (publications)

87 "A Review on Different Image Encryption Approaches", Lecture Notes in Networks and Systems, 2016.

88 < 1% match (publications)
Shi, Jun, Xiaoping Liu, and Naitong Zhang. "Multiresolution analysis and orthogonal wavelets associated with fractional wavelet transform", Signal Image and Video Processing, 2015.

89 < 1% match (publications)
Zhang, Kun Fang, Jian-bo. "Color image encryption algorithm based on TD-ERCS system and wavelet neural network.(Research Articl", Mathematical Problems in Engineering, Annual 2015 Issue

90 < 1% match (publications)
Xue, Wufeng, Lei Zhang, Xuanqin Mou, and Alan C. Bovik. "Gradient Magnitude Similarity Deviation: A Highly Efficient Perceptual Image Quality Index", IEEE Transactions on Image Processing, 2014.

91 < 1% match (publications)
Tao, Ran, Xiang-Yi Meng, and Yue Wang. "Transform Order Division Multiplexing", IEEE Transactions on Signal Processing, 2011.

92 < 1% match (publications)
Saini, Nirmala, and Aloka Sinha. "Video encryption using chaotic masks in joint transform correlator", Journal of Optics, 2015.

93 < 1% match (publications)
Bhatnagar, Gaurav, and Q.M. Jonathan Wu. "A new logo watermarking based on redundant fractional wavelet transform", Mathematical and Computer Modelling, 2013.

94 < 1% match (publications)
Asghar, Mamoona Naveed, Mohammad Ghanbari, and Martin J. Reed. "Sufficient Encryption with Codewords and Bin-strings of H.264/SVC", 2012 IEEE 11th International Conference on Trust Security and Privacy in Computing and Communications, 2012.

95 < 1% match (publications)
Wang, X.. "Hash key-based video encryption scheme for H.264/AVC", Signal Processing: Image Communication, 201007

96 < 1% match (publications)
Hazarika, Nitumoni, and Monjul Saikia. "A novel partial image encryption using chaotic logistic map", 2014 International Conference on Signal Processing and Integrated Networks (SPIN), 2014.

97 < 1% match (publications)
Liu, Zhengjun, She Li, Wei Liu, Yanhua Wang, and Shutian Liu. "Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding", Optics and Lasers in Engineering, 2013.

98 < 1% match (publications)
Asghar, Mamoona Naveed, Mohammed Ghanbari, Martin Fleury, and Martin J. Reed. "Analysis of channel error upon selectively encrypted H.264 video", 2012 4th Computer Science and Electronic Engineering Conference (CEEC), 2012.

99 < 1% match (publications)
Singh, Kehar, G. Unnikrishnan, Naveen K. Nishchal, and Ruyan Guo. "", Photorefractive Fiber and Crystal Devices Materials Optical Properties and Applications VIII, 2002.

100 < 1% match (publications)
Min, S.s.. "Optical CDMA system with the least multiple access interference under arbitrary restrictions", Optics Communications, 20031215

101 < 1% match (student papers from 29-Jun-2015)
Submitted to Thapar University, Patiala on 2015-06-29

102 < 1% match (publications)
Dahake, Prashant, and Sonali Nimbhorkar. "Hybrid cryptosystem for maintaining image integrity using biometric fingerprint", 2015 International Conference on Pervasive Computing (ICPC), 2015.

103 < 1% match (publications)
Luo, Yuling, Lvchen Cao, Senhui Qiu, Hui Lin, Jim Harkin, and Junxiu Liu. "A chaotic map-control-based and the plain image-related cryptosystem", Nonlinear Dynamics, 2015.

104 < 1% match (publications)
Bhatnagar, Gaurav, Q.M. Jonathan Wu, and Balasubramanian Raman. "Discrete fractional wavelet transform and its application to multiple encryption", Information Sciences, 2013.

105 < 1% match (publications)
Lars R. Knudsen. "Using Block Ciphers", Information Security and Cryptography, 2011

106 < 1% match (publications)
Lin Zhang. "Image Encryption with Discrete Fractional Cosine Transform and Chaos", 2009 Fifth International Conference on Information Assurance and Security, 08/2009

107 < 1% match (publications)
Lecture Notes in Computer Science, 2009.

108 < 1% match (publications)
Advances in Intelligent Systems and Computing, 2016.

109 < 1% match (publications)
Pareek, Narendra K., Vinod Patidar, and Krishan K. Sud. "Diffusion–substitution based gray image encryption scheme", Digital Signal Processing, 2013.

110 < 1% match (publications)
Li, Shujun, Guanrong Chen, and Xuan Zheng. "Chaos-Based Encryption for Digital Image and Video", Internet and Communications, 2006.

111 < 1% match (publications)
Tedmori, Sara and Al-Najdawi, Nijad. "Lossless Image Cryptography Algorithm Based on Discrete Cosine Transform", International Arab Journal of Information Technology (IAJIT), 2012.

paper text:

IMAGE AND VIDEO SECURITY USING FRACTIONAL TRANSFORM AND MULTIMODAL BIOMETRIC KEYS A

9**Dissertation Submitted in Partial Fulfillment of** the Requirement **for the Award of** the **Degree of MASTER OF ENGINEERING IN ELECTRONICS AND COMMUNICATION ENGINEERING Submitted By** JOBANPREET KAUR REG. **NO.** 801561010 **Under** Supervision **of Dr.** Neeru Jindal Dr. **Sanjay Sharma** Assistant **Professor,**

8**ECED** Professor, ECED **Thapar University, Patiala** Thapar University, Patiala **ELECTRONICS AND COMMUNICATION ENGINEERING** DEPARTMENT **THAPAR UNIVERSITY, PATIALA,**

8**PUNJAB JULY,** 2017 **i DECLARATION I,** Jobanpreet **Kaur hereby** to **declare that** this **work presented in** this **thesis entitled**

"Image and video security using fractional transform and multimodal biometric keys" in

14**fulfillment of the** requirement **for the award of degree of Master of Engineering submitted** at Electronics **and** Communication **Engineering, Thapar University, Patiala is** genuine **record of work carried out under supervision of**

Dr. Neeru Jindal (Assistant Professor, Thapar University) an d Dr. Sanjay Sharma (Professor, Thapar University). The