A ROBUST AND SECURE REVERSIBLE DATA EMBEDDING ALGORITHM

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted by

DIVYA ARORA

(Roll No. 801633003)

Under the supervision of:

Dr. Anil Kumar Verma

Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY

PATIALA – 147001

JULY 2018

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "A Robust and Secure Reversible Data Embedding Algorithm", in partial fulfillment of the requirements for the award of degree of Masters of Engineering in Information Security submitted in Computer Science and Engineering Department of Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Anil Kumar Verma and other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any degree of this or any other University.

(Divya Arora)

(801633003)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Anil Kumar Verma)

Professor, CSED

ACKNOWLEDGEMENTS

I am truly thankful to my advisor Dr. Anil Kumar Verma and Mr. Maninder Singh, HCSED whose encouragement and guidance at every step enabled me to develop an understanding of the subject. I am grateful for his patience, time and support that he showered on me throughout the length of my research. I am equally thankful to the entire faculty members of CSED for their direct and indirect help and cooperation.

Last but not least, I would like to thank my parents and friends for their encouragement and support. They have always wanted the best for me and I admire their determination and sacrifice. Above all, I would like to thank the Almighty for the kindness who blessed me during this journey.

(Divya Arora)

ABSTRACT

Data security is considered vital as leakage of confidential information (privacy) is a major concern now-a-day. Reversible data hiding is one of the technique(s) to preserve privacy. In the proposed work, the robustness and security concerns has been tackled to make sure the information is not stolen or corrupted. Security is ensured at every level with image encryption, subsampling of image and with strong data embedding algorithm. The proposed work combines the work of cryptography and data hiding into the image. The presented work maintains the privacy and thus providing security of data. The method comprises of three different steps namely, image encryption followed by sampling of image and data embedding. By making use of Lagrange's polynomial the data and image are segregated. The results show that the cover image is extracted without any distortion.

Keywords: *Image encryption, Reversible Data Hiding, Lagrange's interpolation, Image sampling, Data Embedding*

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
DE	Difference Expansion
HS	Histogram Shifting
IDWT	Inverse Discrete Wavelet Transform
LSB	Least Significant Bit
MATLAB	Matrix Laboratory
SL	Multi Security Level
NPCR	No of Pixel Changing Rate
PNG	Portable Network Graphics
PSNR	Peak Signal to Noise Ratio
RDH	Reversible Data Hiding
RHM	Recursive Histogram Modification
SPN	Substitution Permutation Network
XOR	Exclusive OR

CHAPTER 1

INTRODUCTION

1.1 Overview

Data Security is a major concern now-a-days since every information is transmitted through an insecure medium i.e. Internet. In the branch of Information security, Steganography is one of the main pillar for hiding the data especially in the research area. Steganography is the technique of exploiting the property of image to conceal the data within the host image. But hiding data within cover image is just not an option, privacy of data is also a major concern. In order to safeguard, before transmission, data is being encrypted using various techniques of cryptography.

In the past few years, data security is main public concern because of global surveillance. To protect the data and to manage its privacy, many techniques are required. Encryption is one of the key technique for protecting data and convert it in an encrypted form [3,4]. As the data is the encrypted form, the attackers cannot predict the actual text hence data is preserved. Another approach is data hiding, in which the data is hidden into cover text or image. Data embedded doesn't change much of the visual quality of the cover image therefore, stegno image is almost same as the cover image. Therefore, attacker will not be able to understand whether data is being hidden or not, hence, data protection is done.

Steganography [5] is one of the key technique to hide data when it comes to field of information security. The motive is to hide the secret data within the host image by using properties of the image [6,7]. But hiding data within cover image is just not an option, privacy of data is also a major concern. In order to safeguard the data before transmitting it, cryptographic techniques are used to modify it.

Now-a-days, data hidden is vulnerable encrypted by these techniques with considerable increase in computing powers of modern computers. To protect digital media over the insecure medium, data hiding techniques is one of the solution. Steganography and Cryptography, together, made a strong base for any algorithm. The ultimate goal of the network world is to transform the data and secure it from accidental/intentional unauthorized access, this is where the data hiding role comes into play.

There are two methods for data hiding in an image: Reversible and Irreversible. The cover image is exactly extracted with the hidden data in RDH method. No distortion in the cover image as well as in the hidden data. Therefore, RDH is a lossless technique of hiding the data into any image. In irreversible data hiding, only information hidden can be exactly restored but not the cover image in which data is being hidden. The cover image will be distorted and cannot regain its original pixels. Therefore, irreversible data hiding is lossy technique of hiding data in an image.

Achieving reversibility with security goals in the data hiding scheme is still a challenge since it needs good visual quality and high embedding capacity. To ensure reversibility, security, robustness and stenographic protection, designing an algorithm for data hiding system is a task. Even when the hidden data is recovered, recovering the host image is also important i.e. "Image Reversibility". Requirement is to recover the entire image without any distortion.

1.2 Motivation

The main aim is to achieve reversibility and to enhance security in data hiding techniques. Data security provide security to the databases and other confidential information from the unauthorized access. It also protects the data from being corrupted by any unauthorized medium. Reversible data hiding is a one of the data hiding techniques where the host image can be extracted exactly. Being lossless makes this technique suitable for medical and military applications.

Data needs to be transmitted to communicate but since there are chances that data can be stolen or leaked as it is being transmitted in the insecure medium, i.e. internet, it is a challenge to send the data in such a manner that their security is preserved**.**

1.3 Data Hiding

Data hiding [8] hides data for the security purposes into the digital media. Digital image is one of the best way or capsule to hide, store and embed data. Digital Image act as an envelope that provides large capacity to hide and store the information which results into stegno-image which doesn't allow human to recognize in a general manner, basically it's an approach based on data hiding method using steganography as a technique.

Reasons behind to hide and secure data:

- ❖ Personal or private information
- ❖ Sensitive information

❖ Confidential documents

❖ Trade secrets

❖ To avert misuse of data

❖ Accidental deletion or any human error that can cause any unintentional damage to the data

❖ To blackmail or demanding any significant document for any purpose

❖ To hide the crime and all its traces.

❖ Just for fun.

Data Hiding Techniques can be classified as:

❖ Reversible Data Hiding,

Reversible Data Hiding is a one of the data hiding techniques whereby the host image can be recovered exactly.

❖ Irreversible Data Hiding

Irreversible Data Hiding means once the covert image embedded on the actual or cover image, the host image is lost i.e. from stegno image. The actual image cannot be recovered in extraction process.

1.4 Reversible Data Hiding

"Reversible Data Hiding scheme" [9] is the scheme that allows data to be embedded inside an image and then the embedded or stored data can be recovered as needed and the exact actual host image is retrieved as it is. The traditional reversible data hiding schemes are based on modulo arithmetic additive and spread-spectrum techniques.

"Reversible Data Hiding" (RDH) techniques are the one which helps in the lossless embedding of data into the images in such a way that the embedded data can be recovered exactly with the host image restored in the actual format.

Steps to be followed in RDH scheme:

❖ Data Embedding

❖ Data Extraction

To embed the data in the image we need these inputs:

❖ The data that is needed to be embedded i.e. secret data.

❖ The cover data (cover image or host image)

❖ The key.

By combining these inputs, an algorithm is proposed which can produce a stegno image (stegno cover) that can be stored or transmitted. At the receiving end, the receiver or the decoder or the extractor decodes the stegno image and extracts the hidden data and original cover image. In some algorithms at the receiver end, decoder only check whether there is hidden data in the image or not. It is the case where the hidden data are a watermark originally placed in the cover to prove ownership.

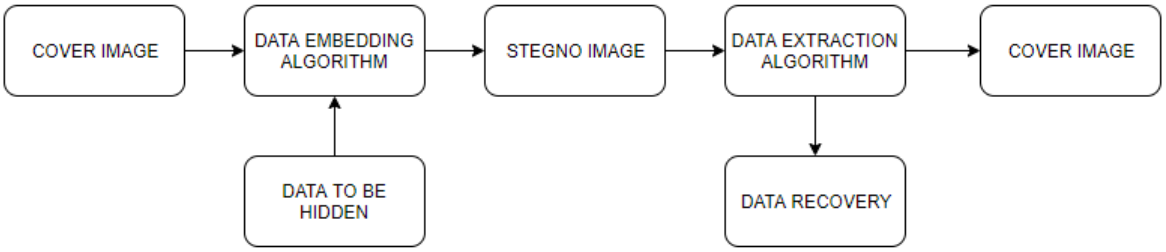


Fig 1.1: RDH Scheme

The important metrics to determine the performance of reversible data-embedding algorithm are

❖ Limit of payload capacity: determines the maximal amount of information that can be stored into the image

❖ Visual quality: determines how much an image is changed after the embedding the data.

❖ Complexity: determines the complexity of the proposed algorithm.

Main focus of RDH scheme is its property- Reversibility - one can remove the embedded data from the stegno image to retrieve the actual or cover image.

And, the main motivation in Reversible Data Hiding Scheme is: distortion-free data embedding. The cover image can be recovered in an exact manner along with the data hidden.

1.5 Techniques in Reversible Data Hiding Scheme

Reversible Data Hiding broadly classified into:

❖ Compression schemes

Initially, the RDH schemes are based on lossless compression [10]- [17] which focused on high capacity embedding or fragile authentication. These schemes focus on the concept of spaces by lossless compressing a subset I which actually belongs to the original host image, and then the space is utilized to embedded or store information. The operation of embedding the information is performed by replacing I with the compressed form Ic, and the message, and so the maximum embedding capacity becomes I-Ic. The performance is evaluated by the selected subset and the employed compression algorithm.

Compression scheme is further divided into:

- Early lossless compression-based scheme
- Recent lossless compression-based scheme

❖ Difference expansion schemes

In [18], [19], Tian proposed an RDH method of high capacity which was based on difference expansion (DE). In DE, to derive the difference values, HAAR wavelet transform is being used to transform the cover media and then for data embedding in a reversible manner, the obtained difference values are used and expanded, to create vacancies. Steps of Tian's DE method:

- For a pixel pair (a, b), their integer average and difference is defined as avg= $\lfloor$(a+ b)/2$\rfloor$ and d = b− a .
- Difference d is expanded to d $*$ = 2d + m , to embed 1 bit $m \in \{0, 1\}$ and keeping the integer average unchanged.
- On the basis of the newly produced difference value d $*$ and original integer average value avg, the marked pixel pair is calculated. Pixel pair (g,f) is calculated as shown in 1:

$$\{ g = avg - \lfloor d* /2 \rfloor \quad f = avg + \lfloor (d* + 1)/2 \rfloor \qquad \ldots 1$$

By reduction as shown in 2, $\{ g = 2a - \lceil (a + b)/2 \rceil \quad f = 2b - \lceil (a + b)/2 \rceil + m$ …2

The original pixel pair (a,b) can be retrieved from the embedded bit m determined from the LSB of f-g as shown in 3

$$\{ a = avg' - \lfloor d' /2 \rfloor \quad b = avg' + \lceil d' /2 \rceil \qquad \ldots 3$$

From the marked pixel pair, avg′ = $\lfloor$(g + f)/2$\rfloor$ and d ′ = $\lfloor$(f − g)/2$\rfloor$ are computed. By DE, one bit can be embedded in pixel pair so its embedding rate becomes 0.5 bpp. To handle the

overflow/underflow problem, Tian adopted a location map which records the selected expandable locations.

❖ Histogram shifting schemes

In [20] and [21], first time, histogram shifting technique is introduced by Ni. In this approach, a histogram is obtained initially, and then the generated histogram properties is being exploited and altering it to embed the data which is actually reversible in nature. In the following way, for a given integer r, the data which is needed to be hidden is embedded into the cover image P to get the embedded image M which is shown in 4.

$$M(m,n) = \begin{cases} P(m,n) - 1, & if\ P(m,n) < r \\ P(m,n) - m, & if\ P(m,n) = r \\ P(m,n), & if\ P(m,n) > r \end{cases} \quad \ldots 4$$

where to be embedded bit is $m \in \{0, 1\}$ and (m,n) represents the pixel coordinate in the cover media. In this scheme, the PSNR of the embedded image versus the actual one is 48.13 dB since every pixel value is being changed by at most 1. In the interest of maximizing the capacity, the integer r can be used as the histogram peak. The embedded data can be extracted and the original media could be restored on the decoder side. By following the steps:

- If M(m,n)< r − 1 , then there is no data which is embedded in the pixel, and the original value is M(m,n) +1.
- If M(m,n) ∈ {r −1, r}, the pixel carries secret data and the embedded bit is m = r – M(m,n).
- If M(m,n) > r, the pixel remains unchanged during embedding operation.

In [22], Fallahpour and Sedaagi proposed block-based histogram shifting in which instead of using the whole image, histogram shifting should be applied to image blocks. In this technique, the host image is first partitioned into multiple blocks. Then, the histogram is produced for individual divided blocks and then for data embedding, Ni et al's histogram shifting is used. With a reduced embedding distortion, the embedding size can be increased. In [23], Lee et al, planned a brand-new technique that uses the bar graph that works on the worth distinction. during this approach AN improved performance is obtained since the spacial correlation of natural image is exploited. Since the distinction bar graph has Laplacian-like distribution and has higher peak points therefore it's treated to be higher for RDH. In [24], X.Li planned a general construction for coming up with the HS-based RDH. This enclosed schemes with special key points. During this technique, the cover image is split into non-overlapping blocks and every block contains n pixels. By tally the

return of every divided block, a n -dimensional bar graph is generated. within the last the information embedding is finished by modifying the n-dimensional bar graph. The element blocks square measure components of $Z\ n$ that is split into disjoint sets. The enlargement supported predefined embedding operate technique is familiar with carry the key knowledge in one set and supported the predefined shifting function; the opposite set is just shifted and is finished to form free areas that guarantee changeableness.

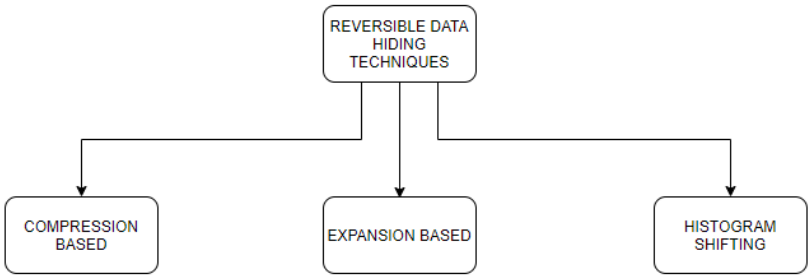


Fig 1.2: Reversible Data Hiding Techniques

1.7 Image Encryption

To ensure data transmission in a secured manner, knowledge is encrypted to undecipherable formats by associate unauthorized person. Cryptography is the essence of information security that has become a really crucial facet of recent computing systems towards data transmission in a secured manner and storage. The interchangeable digital knowledge in cryptography ends up in different algorithms which will be characterized into 2 cryptanalytic mechanisms: regular key within which same secrets used for coding and coding and uneven key within which different keys are used for coding and coding. uneven key algorithms are a lot of secured when put next with regular key algorithms. In today's scenario, data security is based totally on knowledge storage and transmission. pictures are broadly speaking utilized in various processes. As a result, the protection of image knowledge from unauthorized access is crucial at the hands of user. Image coding plays a big role within the field of data concealment. Image concealment or coding ways and algorithms ranges from easy spacial domain ways to a lot of sophisticated and reliable frequency domain.

In the past decade, image encoding is given a lot of attention in analysis of data security and plenty of image encoding algorithms are introduced. as a result of some intrinsic options of pictures like

bulk information capability and high information redundancy, the encoding of image is completely different from that of text; so, it's troublesome to handle them by ancient encoding strategies.

1.7 Techniques of Image Encryption

Techniques are:

- ❖ Image Encryption by XOR and Affine Transform Operation (2011)
- ❖ A New Chaotic System for Image Encryption (2012)
- ❖ A Method for Image Encryption based on One-dimensional Random Scrambling (2012)
- ❖ An Encrypted Image Security Method (2012)
- ❖ Approach for Image Encryption with novel cryptographic technique (2012)
- ❖ An Image Encryption Algorithm Based on Multi-Dimensional Chaotic System and Pixels Location (2012)

1.8 Image Encryption Techniques Comparison

There are many techniques of Image Encryption mentioned and their comparison is carried out in the tabular manner.

Table 1.1 Image Encryption Techniques Comparison

s.no.	Authors	Technique	Key size	Key sensitivity	Entropy		Histogram	Interrelationship between		NPCR %
					Original	Cipher		Original	Cipher	
1	A. Nag, J.P. Singh, S. Khan, S. Biswas et.al [55]	Transformation & XOR	2^64	Low	6.07	7.05	Not good	.3232	.0381	0 (negligible)

2	Long Bao and Yicong Zhou [56]	Three one-dimensional chaotic map	2^240	Very High	7.55	7.96	Good	.9212	.0031	99.61
3	Qiudong Sun, Ping Guan, Yongping and Yunfeng Xue [58]	One dimensional random scrambling	Not fix	High	7.63	7.63	No change (same as original image)	.1915	.0059	99.36
4	Mohammed Abbas and Fadhil AlHusainy [59]	Bit level permutation, XOR & rotation	Not fix	High	7.75	7.99	Good	.5605	.0041	0 (negligible)
5	Nidhi Sethi and Deepika Sharma [60]	Two-dimensional logistic map & compression	10^112	High	7.65	7.98	Good	.9368	.0182	0 (negligible)
6	Hazern Mohammad Al-	Multidimension chaotic function	10^45	High	7.56	7.99	Good	.9462	.01542	99.63

	Najjar [61]									

CHAPTER 2

LITERATURE SURVEY

In this chapter, a brief literature survey on the topics included in this work is presented.

2.1 Error-free Reversible Data Hiding with high capacity in Encrypted Image.

Zhenjun Tang et .al [1] in "Error free reversible data hiding with high capacity in encrypted image", proposed an algorithm with reversible data hiding technique that ensures high data embedding in encrypted image in PNG format by exploiting properties of alpha channel. The algorithm works in certain segments in which secret data is divided and hidden. LSB of the pixel value (encrypted one) is used to hide the one bit and other elements corresponding to it of alpha channel are used to hide other bits, this works for every segment. These segments are then encrypted by 2 chaotic maps. The proposed algorithm works in a perfect manner recovering the secret data with high hiding capacity and visual quality using alpha channel.

2.2 Reversible data hiding scheme using sub-sampled image exploiting Lagrange's interpolating polynomial

Biswapati Jana et .al [2]in "Reversible Data Hiding scheme using sub sample image exploiting Lagrange's interpolating polynomial", proposed a technique in RDH scheme where sub sampled interpolated image and LaGrange's interpolating polynomial is used. At first, sub-sampled images are generated and the its size is increased using interpolation. Now, the secret message is converted into new one and embedded into the blocks using Lagrange interpolating polynomial. The message is divided and hide into the pixels of the blocks from the interpolated image. From each subsampled block, the hidden message is obtained at the receiver end and then Lagrange's interpolation is used to get the equation using the extracted information to retrieve the original message. Data is being hidden within multiple blocks in a distributive manner, hence security is enhanced. During the process of data embedding, the original value of the pixel is not changed that guarantees the reversibility of algorithm. When compared with other techniques of reversible data hiding, this algorithm provides better results in terms of embedding capacity, security and its visual quality.

2.3 Early lossless compression-based scheme

In [10], Friedrich et al., introduced two methods for lossless authentication watermarks. In the first method, lossless compression is done on the selected original LSB's of middle-frequency coefficients and in the same coefficients hash value of the complete image is inserted. In the second method, from the quantization table one quantization coefficient is selected and is changed to half of its value, and to keep the image appearance unchanged all respective coefficients in all blocks are multiplied by two. In the modified coefficients simple LSB embedding is used which reversibly embeds the message or the hash value.

In [12], R-S scheme is explained by Golian. In this technique, the original grayscale image is segmented into disjoint groups, a discrimination function f(d) is also defined which captures the smoothness of the group of pixels and categorizes them as Regular, Singular and Unstable. An invertible operation F(i) called "flipping" is characterized, which permutes the gray levels. Prior to the embedding operation, the groups are scanned and the status is lossless compressed i.e. the RS-vector. In the compressed R-S vector, the message is being appended as bits and the resulting bits stream is stored in the image. In [13], Xuan et al, proposed invertible data embedding technique. This technique makes use of the integer wavelet transform which is using mapping between integer to integer; and arithmetic coding, in the middle and high-frequency sub bands. In the sub bands the binary bits in the chosen bit-plane of the IDWT coefficients are compressed in a lossless manner, even after the algorithm is revealed there is a secret key function that makes the data secret and preprocessing which prevents possible overflow.

In [17], Celik et al, presented a low-distortion, high capacity, Type-II (modified data bits are stored) lossless data embedding algorithm. Instead of the bit planes, this technique alters the main signal at the lowest level to enter or add the embedding data. This generalization gives a finer capacity-distortion granularity. The generalized LSB modifies the raw pixels values as the signal features. The retrieval of the original media is performed by compression, transmission and extracting these features.

2.4 Recent lossless compression-based scheme

In RDH, the payload's upper bound can be embedded in the reversible manner in the host image, for a given distortion constraint. The above constraint in the scheme has been resolved by Kalker

and Willems [25], they developed a different RDH rate-distortion problem, and got the upper bound under a given distortion constraint Δ as shown in 5:

$$\rho re(A) = \max\{G(y)\} - G(x) \quad \ldots 5$$

where ρre is the embedding capacity, x and y are the covers and marked sequence, and G is the entropy function. The distortion constraint is shown in 6:

$$\sum JX\ x.y\ (x)JY\diagup X\ (y\diagup x)\ K(x, y) \leq \Delta \quad \ldots 6$$

where, JY|X(y|x) is the probability matrices and K(x, y) is the square error distortion. In [26]-[32] an asymptotic approach for the rate-distortion on lossless-compression RDH methods is discussed. All the above methods are improved variant of recursive code construction [25]. Recursive histogram modification (RHM) is practiced for lossless compression-based scheme. Firstly, RHM solves the problem for estimating the optimal probability transition matrix JY|X(y|x) and JX|Y(x|y). Secondly, RHM embeds the message recursively into disjoint and small blocks which is created by dividing the cover sequence then modifies the histogram of each block. The codes that approaches the capacity of embedding minimize the distortion caused by embedding for any cover sequence and given payload. Then the designers of RDH only need to concentrate on the formation of a cover signal having small entropy. For a short-sized cover sequence, the entire cover signal cannot be perfectly recovered, in another word, perfect lossless compression cannot be gained.

2.5 Image Encryption by XOR and Affine Transform Operation

A new technique is introduced that uses 64 bit key for encryption purpose by Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar [33]. At the first stage, the proposed algorithm works with the affine transformation to disperse the pixel by using the four subkey of 8 bits. After that, the image is sampled into 2*2 blocks according to the algorithm and thereafter, XOR operation is operated on each block with 4 subkeys of 8 bits to change the pixel value as needed. Figure 2.1 illustrates a host image. The proposed technique works with the transformation operation on the actual or cover image and transformed image is what we get. After that, introduced technique used the XOR operation on the image after transformation operation to get an image which is in a ciphered form. Figure 2.1 illustrate the

original; figure 2.2 denotes the transformed image and figure 2.3 shows the encoded image. Figure 2.4 and 2.5 represents histogram of the first and the transformed image respectively.

Fig 2.1: Car

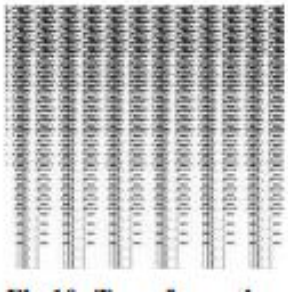


Fig 2.2: Transformation operation

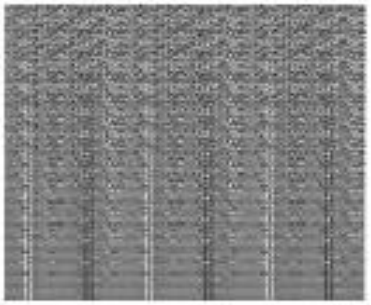


Fig 2.3: Encrypted Image after XOR Operation

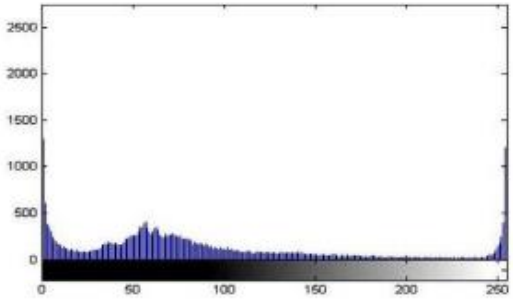


Fig 2.4: Histogram of Image (fig 2.1)

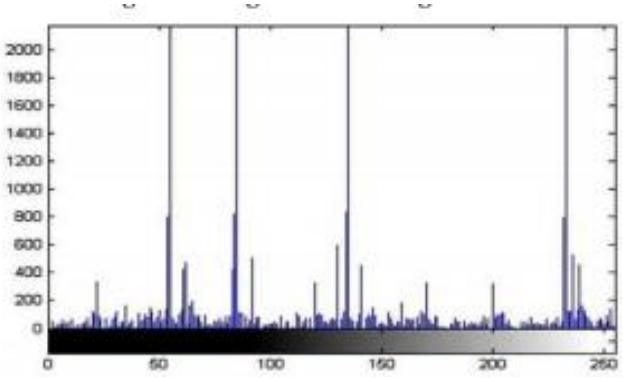


Fig 2.5: Histogram of Encrypted

The above method which is being presented is not that effective in minimizing the interrelationship between the pixel vales and the key space which is used is also short. Hence, the consequences are as such that this algorithm doesn't provide that level of complexity which is required to be used in the encryption process. Therefore, this technique does not provide the strong base to the security to the images because of the key used as it is shorter in length and using simple XOR operation.

2.6 A New System for Image Encryption

A new chaotic system has been introduced by Long Bao and Yicong Zhou [34] which are having the three-distinct one-dimensional chaotic maps. This technique is being used to generate random sequences to choose the tent map or a sine map which uses logistic map as a controller. Therefore, to get the confusion and diffusion property [34,35] this algorithm exploits the properties of substitution-permutation network (SPN). This technique uses large key space which is of 240 bits key. Because of the large key space, this key fulfills all the requirements, all the parameters settings are done with the initial values of the newly introduced chaotic system. There are changes in the key for the encryption and decryption because of the excessive sensitivity. The new approach for the image encryption provides a solid backbone for the security purpose and resistant to the brute force attack as well as their sensitivity issue of key with their chaotic behavior.

2.7 A Method for Image Encryption based on One-dimensional Random Scrambling

A one-dimensional random scrambling-based technique [36] has been suggested by Qiudong Sun, Ping Guan, Yongping and Yunfeng Xue. First step in the algorithm is converting the 2-dimensional image into the 1-dimensional one and then further random shuffling will be done on this 1-dimensional vector. Thereafter, we need to generate an encipher image for which we need to perform an anti-transformation function on the shuffled vector. Iterative calculations are not required under this scheme as to produce the best results only one or two iterations or execution of steps are needed. Figure 2.6 represents a host image of dog; after first iteration of the algorithm, an encrypted image is produced by this technique, which is shown in figure 2.7. After operating 2.7 rounds; the encrypted version is obtained, which is shown in figure 2.8. Moreover, figure 2.9 and figure 2.10 shows the histogram of the original image (dog) and the encrypted image respectively.

Fig 2.6: Image of a Dog

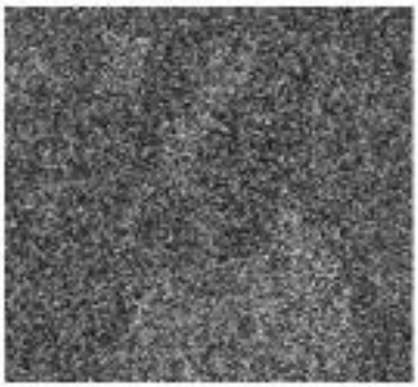


Fig 2.7: Encrypted Image after 1st Iteration

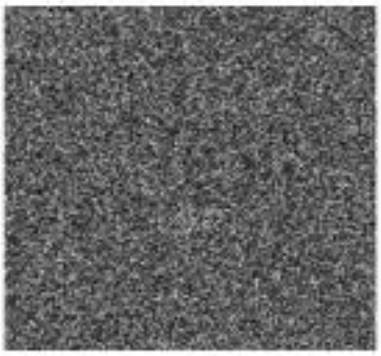


Fig 2.8: Encrypted Image after 15th Iteration

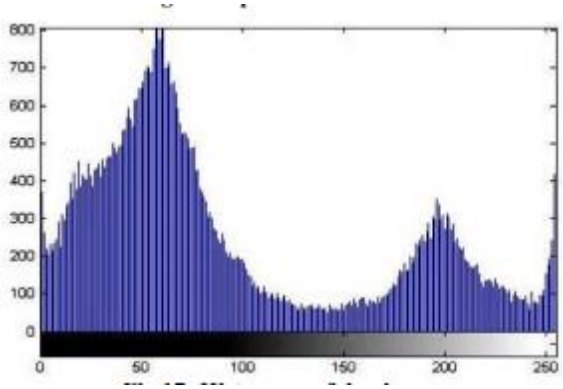


Fig 2.9: Histogram of Dog image

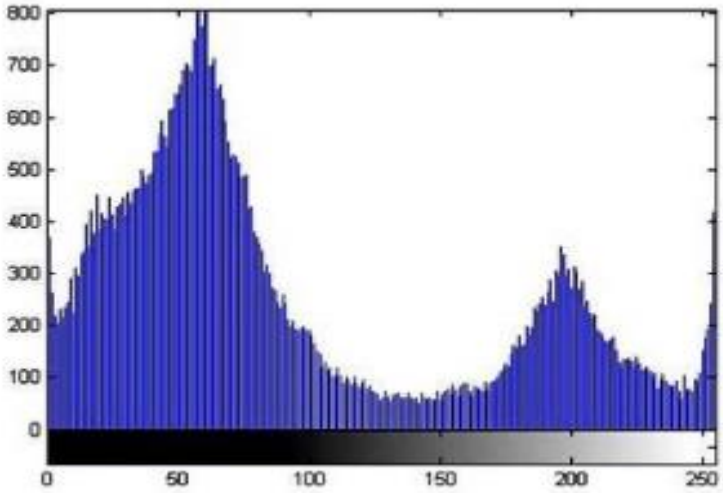


Fig 2.10: Histogram of encrypted Image

After experimenting, due to only scrambling process, it's ascertained that the histogram of the host or an actual image and also image which is being encrypted is same. However, the correlation between pixels is being decreased sue to scrambling process, but it doesn't show any significant changes in the histogram. The proposed scheme is not appropriate for the secret data to be sent or transmit since there is no change in the histogram and histogram of the cipher data can help in revealing the data of the actual image.

2.8 An Encrypted Image Security Method

An approach is being considered on the bit level permutation which is introduced by Mohammed Abbas and Fadhil Al-Husainy [37]. This approach works on the confusion and diffusion properties which is being exploited using two Boolean operation i.e. XOR and pixel bits rotation. In the next step, the algorithm exploits XOR function to the bits of the pixels in the image to encrypt it and further there is a circular rotation of those bits. These steps of XOR and bit rotation is repeated several times to ensure high level of security of confidential data. In this technique, standard secret key is used for both coding and decoding purposes. Figure: 2.11 is a host image, and the figure 2.12 is encrypted image, that differs from the original image completely.

Fig 2.11: Host Image

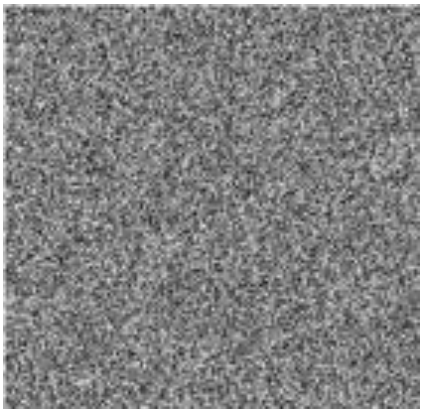


Fig 2.12: Encrypted Image

2.9 Approach for Image Encryption with novel cryptographic technique

An encoding method is suggested by Nidhi Sethi and Dipika Sharma [38], that compresses a picture and using provision mapping to encipher. Initially, Haar wavelet transformation to the picture through which the execution of the whole formula is taken care of. Afterward, 8*8 size blocks from the figure is decomposed to work upon it; then coding process is being operated to

the decomposed image. This encoding scheme has two levels. First, a block-based scrambling is employed to minimize the correlation between inter pixels. The technique depends on the genetic algorithm which uses a crossover approach. In addition to, a 2D Logistic map is used in the scheme to encrypt the pixel values of the image. The encrypted image generated has their confusion and diffusion properties which is being satisfied by the logistic based mode. Afterwards, to ensure the level of security, a key is generated by logistic based mode generated by logistic maps that is needed to be sent to the receiver using watermarking technique.

2.10 An Image Encryption Algorithm Based on Multi-Dimensional Chaotic System and Pixels Location

A new encoding technique has been proposed that relies on the multidimensional chaotic function by Hazern Mohammad Al-Najjar [39]. This scheme focuses on the pixel location and pixel values. This approach basically changes the pixel value and exploit 2 scrambling process which is used to scatter the pixel and for this, 2 substitution strategies are applied on this system. The encryption process of an image is as follows: at the primary level, algorithm uses column index value at first substitution scheme and then based on Rossler equation [39] of X, Y, Z planes is used in method of primary scrambling. Afterward, second substitution scheme is done which uses row index and then shuffling is done exploiting X, Y, Z planes [39]. It is being observed that this algorithm is secure from brute force attack and other types of attack because of the large key size i.e. 10^45 and is sensitive to the initial condition.

CHAPTER 3

RESEARCH PROBLEM

3.1 Problem Statement

As the internet is growing day by day, secure transmission of the data is very crucial. So, secure transmission of information must be secretive as well as secure. Internet communication is essential part of communication now-a-days. So, we can increase the confidentiality of data by applying the security techniques and data hiding techniques to provide more security to the data. When digital information is transmitted over the internet, it can be edited or tampered by the attackers. This problem yields the biggest concern over the last few years. So, the unauthorized access of the transmitted information and ownership of the document needs to be protected.

The proposed work focuses on the security of the data that needed to be transmitted over the insecure medium. Presented work shows the robustness of the algorithm by providing security at different levels. In this work mentioned, cryptographic techniques and data hiding techniques are used to make the algorithm more secure and robust in nature. Image Encryption is used at the first level then image sampling is done along with interpolating the image in which data is being hidden where a data hiding technique is used that works with the Lagrange's polynomial. The main motive of the work done is to make sure the data hidden is exactly extracted along with the cover image in a secure manner.

3.2 Research Gaps

Previous work shows either the data hiding techniques or encrypting the image. Both work together provide the robustness to the system. To provide the robustness and security to the work so that the information hidden cannot be recognized or tampered in any of the case, multilevel security is achieved through the presented work. Multiple single-level or multi-security level (MSL) is a way to establish security at completely different levels of knowledge by exploitation separate computers or virtual machines for every level. It helps and manages to administer a number of the advantages of construction security with none would like of special changes to the OS or

applications, however it adds to the value of needing further hardware. This gap needed to be managed and work need to be done for more secure and robust algorithms.

3.3 Research Objectives

The proposed work provides the following objectives:

1. Combining techniques at different security level to make the technique more strong, secure and robust.
2. Presenting a hybrid technique that allows more level of security
3. Privacy and Integrity is maintained as data can be extracted in an exact manner along with the cover image.
4. Exploring the Reversible Data Hiding Techniques with cryptographic ones.

3.4 Research Methodology

The method of the algorithm includes major 4 steps:

1. Image Encryption

This level of encrypting an image is the first stage from which robustness of the algorithm works.

2. Sub-Sampling of Image

A 4*4 block is taken which is sampled into 4 blocks of 2*2 block.

3. Interpolation

After sampling of image, each 2*2 block is interpolated into 3*3 block. To interpolate the 2*2 block into 3*3 one in MATLAB, interpolate2 function is used

4. Data Embedding Algorithm

To embedded the data into the encrypted image.

CHAPTER 4

DESIGN AND IMPLEMENTATION

In our proposed scheme, we have designed the algorithm which is secure as well as robust. The algorithm is basically a reversible data embedding algorithm which includes multilevel security. The proposed algorithm is hybrid reversible data hiding algorithm in images.

The process how our proposed algorithm work shows in the following flowchart

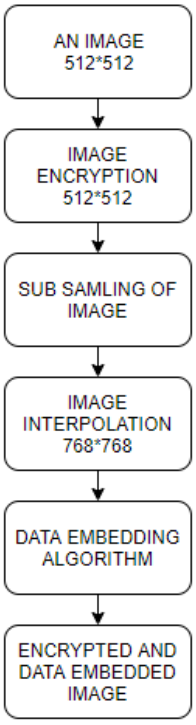


Fig 4.1: Flowchart of Proposed Scheme

Our algorithm works in multiple levels as shown in the above flow chart. Each level has their own properties and its security robustness. Each level adds on the security implications which makes the algorithm more secure and robust.

Now, every stage is described as follows:

1. An Image

A Grayscale Image is considered as the host image in which data will be embedded in a secured manner to transmit.

2. Image Encryption

This level of encrypting an image is the first stage from which robustness of the algorithm works.

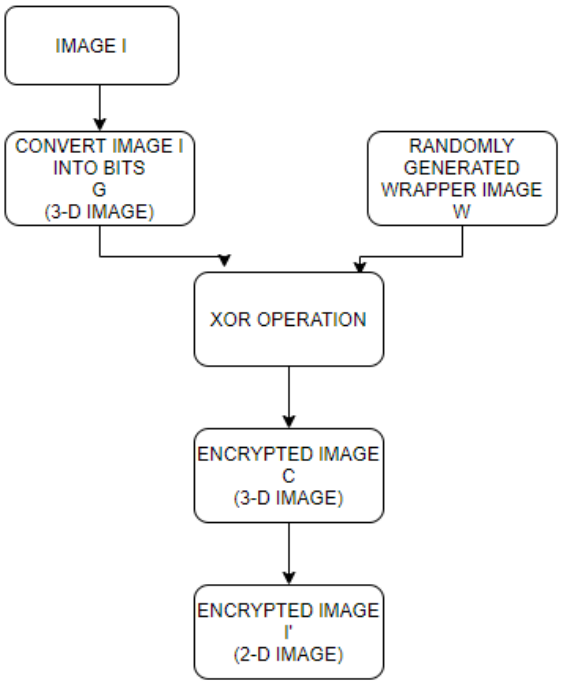


Fig 4.2: Flowchart Showing Encryption of Image

To encrypt the image, follow these steps:

Step 1: Consider an Image I.

Step 2: Convert the image I into bits from integer value as mentioned.

$$G(i,j,k)= \mathrm{mod}(\mathrm{floor}(I(i,j)/2,2)$$

Where, $0 \leq i \leq P$

$0 \leq j \leq Q$

$$0 \leq k \leq 7$$

Step 3: Obtain a wrapper image W randomly generated and secure it with a secret key s.

W(i,j,k), where

$$0 \leq i \leq P$$

$$0 \leq j \leq Q$$

$$0 \leq k \leq 7$$

Step 4: XOR image G and image W and obtain image C

$$C(i,j,k) = G(i,j,k) \oplus W(i,j,k)$$

Where, $0 \leq i \leq P$

$0 \leq j \leq Q$

$0 \leq k \leq 7$

Step 5: The Image obtained C is converted into 2-D image I'.

$$I'(i,j) = \sum 2^k C(i,j,k)$$

Where, $0 \leq i \leq P$

$0 \leq j \leq Q$

$0 \leq k \leq 7$

3. Sub-Sampling of Image

A 4*4 block is taken which is sampled into 4 blocks of 2*2 block as shown

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

1	3
9	11

2	4
10	12

5	7
13	15

6	8
14	16

4. Image Interpolation

After sampling of image, each 2*2 block is interpolated into 3*3 block. To interpolate the 2*2 block into 3*3 one in MATLAB, interpolate2 function is used.

Example:

12	15
16	21

12	13	15
14	16	18
16	18	21

(12+15)/2 =13,

(12+15+16+21)/4=16 and so on.

5. Data Embedding algorithm

To embedded the data into the encrypted image, follow the following steps:

Step 1: Take the secret message M, convert it into ASCII value.

Step 2: Let the ASCII value be a. Assume 2 value y and z as predefined and work with the given polynomial

$$f(x)= zx^2+yx+a$$

Step 3: Now from the encrypted image I', take block of 6*6 and divide into 4 blocks of 3*3

Step 4: Calculate value for f(x) for x=1,2,3,4 for 4 blocks respectively.

For x=1, f(x) is represented in 12 bits format and partitioned into 4 parts, 3 bits each which is then converted into decimal value and further added to the interpolated pixel value. The value of x is added to the middle pixel value.

Example:

Let the message be M.

A= 105 (ASCII value of M)

Let y=5 and z=4

Calculate $f(x)= zx^2+yx+a$

For x=1, f(x) =114

Represent into 12 bits then decimal value of each 3-bit part

000	001	110	010

(12 Bit Representation)

0	1	6	2

(decimal value)

Now take interpolated 3*3 block from the image.

12	13	15
14	16	18
16	18	21

Add the decimal value to the pixel value

13+0=13

14+1=15

18+6=24

18+2=20

16+x=16+1=17

Updated block:

12	13	15
15	17	24
16	20	21

Perform the same procedure for x=2,3 and 4 for block 2,3,4.

For x=2, f(x) =133

Represent into 12 bits then decimal value of each 3-bit part

000	001	000	101

(12 Bit Representation)

0	1	0	5

(decimal value)

Now take interpolated 3*3 block from the image.

15	21	27
17	21	25
20	21	23

Add the decimal value to the pixel value

21+0=21

17+1=18

25+0=25

21+5=26

21+x=21+2=23

Updated block:

15	21	27
18	21	25
20	26	23

For x=3, f(x) =162

Represent into 12 bits then decimal value of each 3-bit part

000	010	100	010

(12 Bit Representation)

0	2	4	2

(decimal value)

Now take interpolated 3*3 block from the image.

19	22	26
21	22	24
23	22	22

Add the decimal value to the pixel value

22+0=22

21+2=23

24+4=28

22+2=24

22+x=22+3=25

Updated block:

19	22	26
23	22	28
23	24	22

For x=4, f(x) =201

Represent into 12 bits then decimal value of each 3-bit part

000	011	001	001

(12 Bit Representation)

0	3	1	1

(decimal value)

Now take interpolated 3*3 block from the image.

21	23	25
22	25	27
24	27	30

Add the decimal value to the pixel value

23+0=23

22+3=25

27+1=28

27+1=28

25+x=25+4=29

Updated block:

21	23	25
25	29	27
24	28	30

6. Encrypted and Data Embedded Image

Embedded each character of secret message on 6*6 block by using the data embedding algorithm through which data is being hidden in the image encrypted.

The image is then send to the receiver in which data is embedded. The hidden data is retrieved at the receiver end by reversing all the steps as mentioned. To recover the hidden data from the image, follow the steps:

Step 1: Take 6*6 block, divide into four 3*3 blocks.

Step 2: Extract the data using interpolation method used by subtracting the obtained and mentioned and then represent them into 12 bits and then again 12 bits to its decimal value.

Step 3: Perform the step 2 for all the four blocks with their corresponding value of x.

Step 4: Use any of the 3 blocks combination to extract the data.

Step 5: Use LaGrange's polynomial method to the quadratic equation and extracting the original ASCII value to the message hidden.

At another level mentioned in the proposed algorithm, the method is reversed to extract the image.

Example:

12	13	15	15	21	27
15	17	24	18	21	25
16	20	21	20	26	23
19	22	26	21	23	25
23	22	28	25	29	28
23	24	22	24	28	30

Extract the 3*3 blocks

12	13	15
15	17	24
16	20	21

15	21	27
18	21	25
20	26	23

19	22	26
23	22	28
23	24	22

21	23	25
25	29	27
24	28	30

Now extract the data from the extracted blocks. Blocks are numbered are Zs1, Zs2, Zs3 and Zs4.

Block Zs1:

12	13	15
15	17	24
16	20	21

Extract data as

$$13-(12+15)/2=0$$

15-(12+16)/2=1

24-(15+21)/2=6

20-(16+21)/2=2

Representation of these in 3 bits each

0	1	6	2

(decimal format)

000	001	110	010

(12 Bit Representation)

Decimal value: (1,114)

Block Zs2:

15	21	27
18	21	25
20	26	23

Extract data as

21-(15+27)/2=0

18-(15+20)/2=1

25-(27+23)/2=0

26-(20+23)/2=5

Representation of these in 3 bits each

0	1	0	5

(decimal format)

000	001	000	101

(12 Bit Representation)

Decimal value: (2,133)

Block Zs3:

19	22	26
23	22	28
23	24	22

Extract data as

22-(19+26)/2=0

23-(19+23)/2=2

28-(26+22)/2=4

24-(23+22)/2=2

Representation of these in 3 bits each

0	2	4	2

(decimal format)

000	010	100	010

(12 Bit Representation)

Decimal value: (3,162)

Block Zs4:

21	23	25
25	29	27
24	28	30

Extract data as

23-(21+25)/2=0

25-(21+24)/2=3

27-(25+30)/2=1

28-(24+30)/2=1

Representation of these in 3 bits each

0	3	1	1

(decimal format)

000	011	001	001

(12 Bit Representation)

Decimal value: (4,201)

Now use Lagrange's polynomial to extract the ASCII value of the hidden message.

Use any one combination of block number out of these four

{(1,2,3), (2,3,4), (1,3,4), (2,1,4)}

Let’s have (1,2,3) as a combination for extracting the message.

$P(x)=(((x-2)(x-3))/((1-2)(1-3))*f(1) + (((x-1)(x-3))/((2-1)(2-3)))* f(2) + (((x-1)(x-2))/((3-1)(3-2)))*f(3)$

$=(x^2-5x+6)(57)-(x^2-4x+3)(133) +(x^2-3x+2)(81)$

$=57x^2-285x+342-133x^2+532x-399+81x^2-243x+162$

$=5x^2+4x+105$

A0=105 (ASCII value of hidden message)

CHAPTER 5

EXPERIMENTAL RESULTS

This algorithm is implemented in MATLAB. Results are shown as:

Fig 5.1
Lena as test image

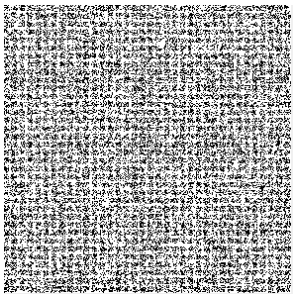


Fig 5.2
Encrypted Lena

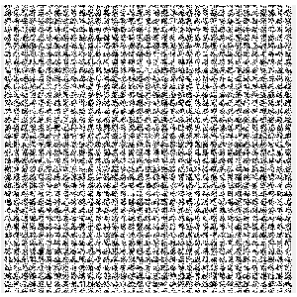


Fig 5.3
Data Embedded in Encrypted Lena

Fig 5.1 shows the gray scale image which is being taken to hide or embedd the data into. Fig 5.2 is the encrypted image. Fig 5.3 show the image in which data is being hidden which is send to the receiver.

Procedure is done as follows:

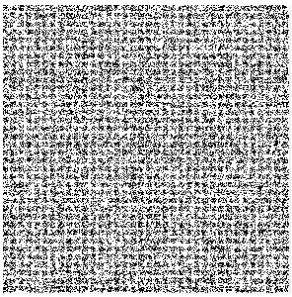
Stepwise procedure is shown with the help of the images

Lena is taken as test image which is first encrypted then secret image is embedded into the message.

After the encryption, data embedded image is send at the receiver end and there secret message is extracted with the original image.

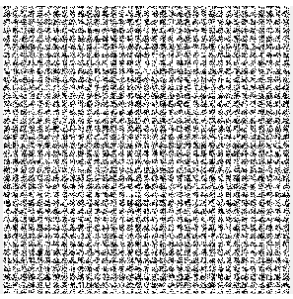
AT SENDER SIDE (**fig 5.4**);

Image taken to encrypt



Encrypted Image

SECRET MESSAGE



DATA EMBEDDED IMAGE

AT RECEIVER SIDE (**FIG 5.5**),

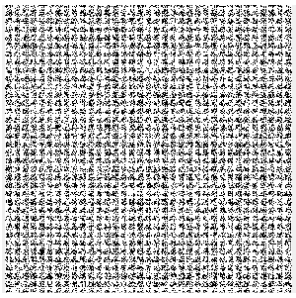
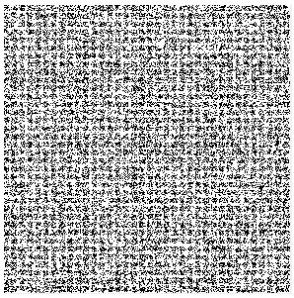


Image transmitted

SECRET MESSAGE



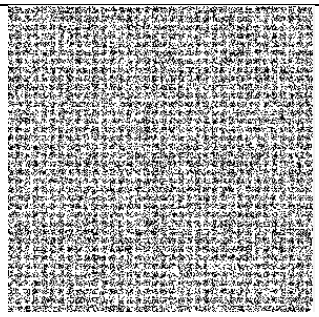
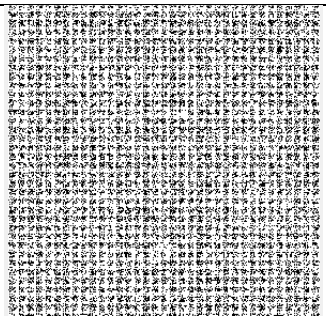
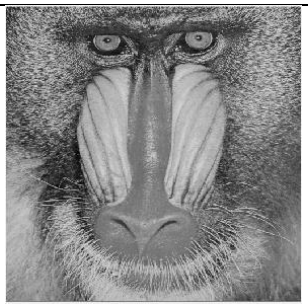
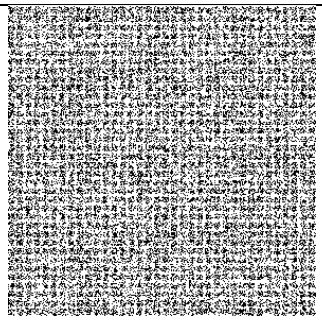
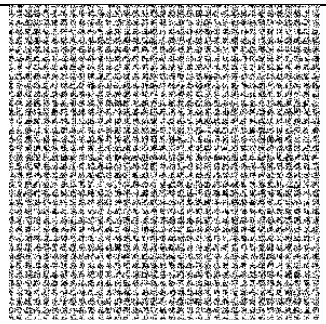
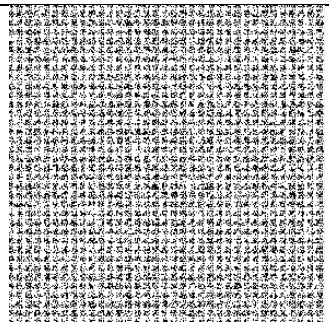
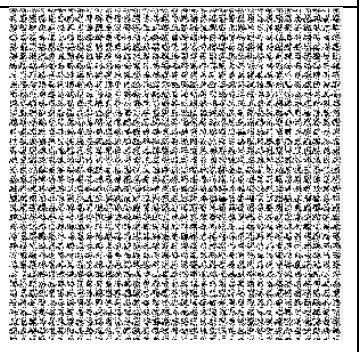
ENCRYPTED IMAGE

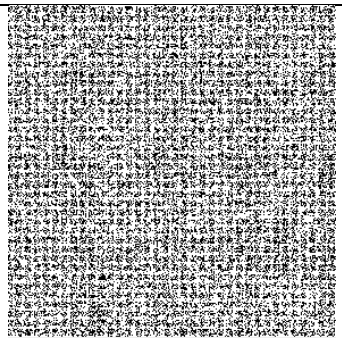
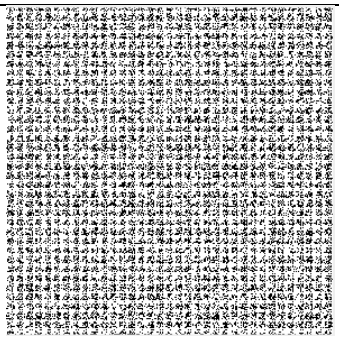
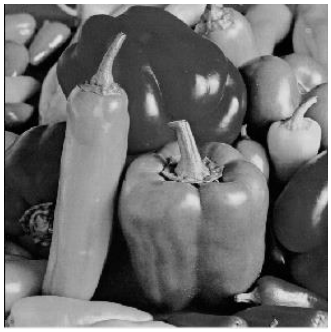
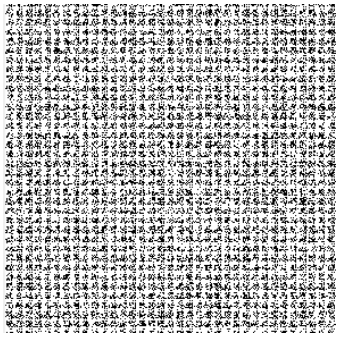
ORIGINAL IMAGE

Similarly, the algorithm has worked with more test images.

Table is shown with test images and their encrypted image and data embedded image.

Table 5.1: Result of algorithm with Test Images

Name of test image	Original Image	Encrypted Image	Data Embedded Image
Lena			
Baboon			
Barbara			
Boat			

Goldhill			
Pepper			

To break this algorithm, one needs to go and face the robustness of algorithm at every level. At first, at the stage of Image encryption, to decrypt the image the complexity is $O(n^3)$ and then, during the process of sub-sampling of image, image is completely distorted from 4*4 block to 4 2*2 blocks which is interpolated and after that data is being embedd into the encrypted image using Lagrange's polynomial.

The advantage of data embedding algorithm is that data is hidden in 4 blocks of 6*6 block of 3*3 block each but it can be retrieved by any 3 of the blocks so even if any of the block is distorted, data can be retrieved but the original image won't be able to recover in exact manner in that case.

The results are achieved in terms of PSNR value when compared two images obtained in the process of proposed algorithm.

Table 5.2: PSNR value of Encrypted Image with Data Embedded Image.

TEST IMAGE	PSNR VALUE (DATA EMBEDDED IMAGE AND ENCRYPTED IMAGE)
LENA	24.7001
BABOON	24.5509

BARBARA	23.9257
BOAT	24.6050
GOLDHILL	24.5920
PEPPER	24.6500

Since it is a RDH scheme, the cover image is extracted in an exact manner at the receiver end. This is shown by comparing the cover image and the image extracted at the receiver end. It can be explained using PSNR value. Since the PSNR value is INFINITE, there is no change in the cover image and the image obtained at receiver end.

Table 5.3: PSNR value of Cover Image with Image Extracted.

TEST IMAGE	PSNR VALUE (COVER IMAGE AND IMAGE EXTRACTED)
LENA	INFINITE
BABOON	INFINITE
BARBARA	INFINITE
BOAT	INFINITE
GOLDHILL	INFINITE
PEPPER	INFINITE

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

From the proposed algorithm, robustness and security of the data hiding within the encrypted image is shown at different level which includes image encryption, sub-sampling of image and data embedding using Lagrange's polynomial. The proposed scheme is robust at each level of which result is being shown in above section. This can further be improved by using different methods of image encryption and data embedding techniques.

The algorithm is designed in such a way that added to the security at each level of it. It not only increases the security of the image but also provide robustness to the algorithm. Its is difficult to break the algorithm at each level. The experimental results are already mentioned with the test images results. The further improvement is explained in the future scope.

The future scope of the presented work may be explored by:

- Increasing the security of algorithm by improving techniques involved.
- Increasing the capacity of data hidden in the stegno image.
- Enhancing the data embedding technique and combining it with more robust technique.
- Increasing the level of steps involved in the algorithm mentioned.
- Experimenting with different kind of data.

REFERENCES

[1] Tang, Zhenjun, et al. "Error-free reversible data hiding with high capacity in encrypted image." OptikInternational Journal for Light and Electron Optics 157 (2018): 750-760.

[2] Jana, Biswapati. "Reversible data hiding scheme using sub-sampled image exploiting Lagrange's interpolating polynomial." Multimedia Tools and Applications (2017): 1-17.

[3] E. Vaferi, R. Sabbaghi-Nadooshan, A new encryption algorithm for color images based on total chaotic shuffling scheme, Optik 126 (20) (2015) 2474–2480.

[4] Z. Tang, X. Zhang, Secure image encryption without size limitation using Arnold transform and random strategies, J. Multimedia 6 (2) (2011) 202–206.

[5] Johnson, Neil F., and Sushil Jajodia. "Exploring steganography: Seeing the unseen." Computer 31.2 (1998).

[6] Fridrich, Jessica, Miroslav Goljan, and Rui Du. "Detecting LSB steganography in color, and gray-scale images." IEEE multimedia 8.4 (2001): 22-28.

[7] Denemark, Tomáš, Patrick Bas, and Jessica Fridrich. "Natural Steganography in JPEG Compressed Images." Electronic Imaging. 2018.

[8] Bender, Walter, et al. "Techniques for data hiding." IBM systems journal 35.3.4 (1996): 313-336.

[9] Zhang, Xinpeng. "Reversible data hiding in encrypted image." IEEE signal processing letters 18.4 (2011): 255-258.

[10] J. Fridrich, M. Goljan, and R. Du, ``Invertible authentication," Proc. SPIE, vol. 4314, pp. 197_208, Aug. 2001. [20] J. Fridrich, M. Goljan, and R. Du, ``Lossless data embedding_New paradigm in digital watermarking," EURASIP J. Adv. Signal Process.,vol. 2002, no. 2, pp. 185_196, 2002.

[11] M. Goljan, J. J. Fridrich, and R. Du, ``Distortion-free data embedding for images," in Proc. 4th Inf. Hiding Workshop, 2001, pp. 27_41.

[12] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, ``Distortionless data hiding based on integer wavelet transform," Electron. Letter, vol. 38, no. 25, pp. 1646_1648, Dec. 2002.

[13] G. Xuan, J. Chen, J. Zhu, Y. Q. Shi, Z. Ni, and W. Su, ``Lossless data hiding based on integer wavelet transform," in Proc. IEEE Int. Workshop Multimedia Signal Process., Dec. 2002, pp. 312_315.

[14] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, ``Reversible datahiding," in Proc. IEEE Int. Conf. Inf. Process., vol. 2. Sep. 2002, pp. 157_160.

[15] G. Xuan et al., ``High capacity lossless data hiding based on integer wavelet transform," in Proc. IEEE Int. Symp. Circuits Syst., vol. 2. May 2004, pp. 29_32.

[16] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, ``Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253_266, Feb. 2005.

[17] M. U. Celik, G. Sharma, and A. M. Tekalp, ``Lossless watermarking for image authentication: A new framework and an implementation," IEEE Trans. Image Processing, vol. 15, no. 4, pp. 1042_1049, Apr. 2006.

[18] J. Tian, ``Wavelet-based reversible watermarking for authentication," Proc. SPIE, vol. 4675, pp. 679_690, Apr. 2002.

[19] J. Tian, ``Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890_896, Aug. 2003.

[20] Z. Ni, Y.-Q. Shi, N. Ansari, andW. Su, ``Reversible data hiding," in Proc. IEEE Int. Symp. Circuits Syst., May 2003, pp. II-912_II-915.

[21] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, ``Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354_362, Mar. 2006.

[22] M. Fallahpour and M. H. Sedaaghi, ``High capacity lossless data hiding based on histogram modification," IEICE Electron. Exp., vol. 4, no. 7, pp. 205_210, 2007.

[23] S.-K. Lee, Y.-H. Suh, and Y.-S. Ho, ``Reversible image authentication based on watermarking," in Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2006, pp. 1321_1324.

[24] X. Li, B. Li, B. Yang, and T. Zeng, ``General framework to histogram shifting- based reversible data hiding," IEEE Trans. Image Process., vol. 22, no. 6, pp. 2181_2191, Jun. 2013.

[25] T. Kalker and F. M. J. Willems, ``Capacity bounds and constructions for reversible datahiding," in Proc. Int. Conf. Digit. Signal Procesing., vol. 1. 2002, pp. 71_76.

[26] W. Zhang, B. Chen, and N. Yu, ``Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991_3003, Jun. 2012.

[27] S.-J. Lin and W.-H. Chung, ``the scalar scheme for reversible information-embedding in gray-scale signals: Capacity evaluation and code constructions," IEEE Trans. Inf. Forensics Security, vol. 7, no. 4, pp. 1155_1167, Aug. 2012.

[28] X. Zhang, ``Reversible data hiding with optimal value transfer," IEEE Trans. Multimedia, vol. 15, no. 2, pp. 316_325, Feb. 2013.

[29] X. Hu, W. Zhang, X. Hu, N. Yu, X. Zhao, and F. Li, ``Fast estimation of optimal marked signal distribution for reversible data hiding," IEEE Trans. Inf. Forensics Security, vol. 8, no. 5, pp. 779_788, May 2013.

[30] W. Zhang, X. Hu, X. Li, and N. Yu, ``Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. Image Processing, vol. 22, no. 7, pp. 2775_2785, Jul. 2013.

[31] W. Zhang, X. Hu, X. Li, and N. Yu, ``Optimal transition probability of reversible data hiding for general distortion metrics and its applications," IEEE Trans. Image Processing, vol. 24, no. 1, pp. 294_304, Jan. 2015.

[32] F. Balado, ``Optimum reversible data hiding and permutation coding," in Proc. IEEE Int. Workshop Inf. Forensics Secur., Nov. 2015, pp. 1_4.

[33] Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar "Image Encryption Using Affine Transform and XOR Operation" 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011), 21-22 July 2011, pages : 309-312.

[34] Long Bao, Yicong Zhou, C. L. Philip Chen, Hongli Liu "A New Chaotic System for Image Encryption" 2012 International Conference on System Science and Engineering, June 30-July 2, 2012, pages: 69-73 .

[35] D. R.Stinson, Cryptography, Theory and Practice. Third edition: Chapman & Hall/CRC, 2006

[36] Qiudong Sun, Ping Guan, Yongping Qiu, Yunfeng Xue "A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling" 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, 29-31 May 2012, page: 1669- 1672.

[37] Mohammed Abbas Fadhil Al-Husainy, "A Novel Encryption Method for Image Security", International Journal of Security and Its Applications, vol.6, no.1, January 2012, pages: 1-8.

[38] Nidhi Sethi, Deepika Sharma, "A New Cryptographic Approach for Image Encryption", Parallel, Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on 6-8 Dec. 2012, pages: 905- 908

[39] Hazem Mohammad Al-Najjar, “Digital Image Encryption Algorithm Based on Multi-Dimensional Chaotic System and Pixels Location”, International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012, pages: 354-357.

APPENDIX A

PUBLICATIONS

[1] Divya Arora and Anil Kumar Verma, "A ROBUST AND SECURE HYBRID REVERSIBLE DATA EMBEDDING ALGORITHM ", in International Conference on Computing, Power and Communication Technologies 2018. (**accepted)**

[2] Divya Arora and Anil Kumar Verma, "PRIVACY PRESERVING DATA MINING TECHNIQUES ", in Machine Learning for Computer and Cyber Security: Principles, Algorithms, and Practices**. (communicated).**

APPENDIX B

VIDEO PRESENTATION LINK

https://www.youtube.com/watch?v=AY4RFg8rh_g

APPENDIX C

PLAGIARISM REPORT

Report

ORIGINALITY REPORT

10%	5%	8%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	research.ijcaonline.org Internet Source	3%
2	Shi, Yun-Qing, Xiaolong Li, Xinpeng Zhang, Haotian Wu, and Bin Ma. "Reversible Data Hiding: Advances in the Past Two Decades", IEEE Access, 2016. Publication	1%
3	www.mai.liu.se Internet Source	<1%
4	www.nd.edu Internet Source	<1%
5	Communications in Computer and Information Science, 2011. Publication	<1%
6	Xiaolong Li, Weiming Zhang, Bo Ou, Bin Yang. "A brief review on reversible data hiding: Current techniques and future prospects", 2014 IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP), 2014	<1%