LSB based Steganography Techniques for Data Transmission Security

A Thesis Submitted in Fulfillment of the Requirement for the Award of the Degree of

Master of Engineering

in

Wireless Communication

Submitted by: Sahil Kaushal

Roll No: 801663005

Under Supervision of

Dr. Ajay Kakkar

Assistant Professor

THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR INSTITUTE OF ENGINEERING & TECHNOLOGY

(A DEEMED TO BE UNIVERSITY), PATIALA, PUNJAB JUNE, 2018

Declaration

I hereby declare that the thesis report entitled "**LSB based Steganography Techniques for Data Transmission Security**" is an authentic record of my study carried out as requirement for the award of degree of ME (Wireless Communication) at Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, under the supervision of Dr. Ajay Kakkar, "Electronics and Communication Engineering Department" during 4th Semester 2018.

10/7/18
Date:

Sahil Kaushal
Sahil Kaushal
801663005

I certified that above statement made by the student is correct to best of my knowledge.

10/7/18
Date:

Ajay
Dr Ajay Kakkar
Assistant Professor, ECED

Acknowledgement

First of all, I would like to express my gratitude to **Dr. Ajay Kakkar**, **Assistant Professor,** Electronics and Communication Engineering Department, Thapar Institute of Engineering and Technology, Deemed to be University Patiala for his patient guidance and support throughout this report. I am truly very fortunate to have the opportunity to work with him. I found this guidance to be extremely valuable. I am also thankful to our Head of Department, **Dr. Alpana Agarwal** and P.G. Coordinator, **Dr. Amit Mishra**. I would like to thank the entire faculty and staff of Electronics and Communication Engineering Department and then friends who devoted their valuable time and help me in all possible ways towards successful completion of this work. I thank all those who have contributed directly or indirectly to this work.

Lastly, I would like to thanks my parents for their years of unyielding love and encourage they have always wanted the best for me and I admire their determination and sacrifice.

Sahil Kaushal

801663005

Abstract

Steganography is a data hiding technique which is used to prevent the data or any relevant information from falling to the hands of an unauthorized personal. So, in order to prevent such scenario the steganographic method is used using LSB matching technique in which the LSB of the pixels of the cover media is replaced with that of the relevant information and the cover media is chosen based on characteristics known to only the sender and receiver and no one else can access it. The steganographic technique can find its relevance and scope in merely many field like Marketing, MNC's, Industry, Medical, Research and Defense etc. Like any other data hiding method it is also based on 3 key parameters: a) Rubustness; how well and unaltered the information is transferred from on e-party to the other. Based on this it is preferred using formats like BMP which are lossless rather than JPEG which are lossy, b) Capacity; how much payload/data can it carry in a single transaction. Ideally the relative payload that an steganographic image can hold is ≈ 1% of the image, so that, it could be undetectable the bigger the media the more is the payload but there is a word of caution a sudden a large exchange of file has chance of suspicion, c) Security; how securely the data can be transferred from one party to other. The literature review has been done by keeping in mind to obtain ideas and techniques to detect and improve as much as possible to the steganographic techniques and through research and work done on MATLAB software, were able to detect LSB based steganographic encrypted image from the others. To this some remarks were added to improve the security and evident in result section.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

LSB	Least Significant Bit
HVS	Human Visual System
HTML	Hyper Text Markup Language
EXE	Executable File
XML	Extensible Markup Language
ID	Identification
GIF	Graphic Interchange Format
JPEG	Joint Photographic Expert Group
PNG	Portable Network Graphics
BMP	Bitmap Format
DCT	Discrete Cosine Transformation
FT	Fourier Transformation
DWT	Discrete Wavelet Format
TCP	Transmission Control Protocol
IP	Internet Protocol
HSV	Hue Saturation Value
MNC	Multi National Corporation
QR	Quick Response
JAN	Japanese Article Number
PM	Perceptual Masking
AS	Adaptive Steganography
UC	Universal Composability
CT	Cipher Text
RPM	Random Phase Mark
PEKs	Public Key Encryption with Keyword Search
KGA	Keyword Guessing Attack
PVD	Pixel Value Difference
DPSK	Differential Phase Shift Keying
CSK	Code Shift Keying
PPKI	Pseudonymous Public Key Infrastructure
DHCF	Difference Histogram Characteristic Function
DHCFM	Difference Histogram Characteristic Function Moment
PVD	Pixel Value Differaence

EA	Edge Adaptive
WOW	Wavelet Obtained Weights
HUGO BD	Highly Undetected Stego Bounding Distortion
S-UNIWARD	Spatial Universal Wavelet Relative Distrotion
ASO	Adaptive Steganography by Oracle
PSRM	Projection Spatial Rich Model
FLD	Fisher Linear Discriminant
SRM	Standard Response Measure
UED	Uniform Embedding Distortion

Chapter 1
INTRODUCTION

1.1 Introduction: Following are some of the basic concepts that one should understand carefully and be familiar with before proceeding further in the field of cyber security, encryption and embedding technique. The definitions are as follows:

Security system: The most basic definition of a security system can be defined as a system which is responsible for providing and maintaining the security measures for any system to whom it is assigned to or responsible for example home security system, car security system etc [3].

Cryptography: It can be referred as an art or technique of hiding any form of important data or information from being assessed by any unwanted or unauthorized user. The encrypted text is known as cipher text, and in order to retrieve the text back the receiver needs the key which is only meant to be shared with the authorized users as shown in figure 1.1 [100]. During this process data or information is encrypted into cipher text format with the help of the a secret key, and the secret key is only shared with only the authorized person so that only they are able to decrypt the data or information using the same key which is used to encrypt the data or information [100].

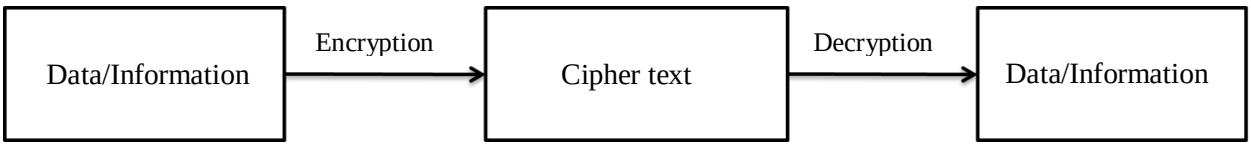


Figure 1.1: Block diagram defining basic concept of Cryptography

Types of Cryptography: The cryptographic technique is broadly classified in 3 main types and described as below:

- **Asymmetric Key Cryptography**: This is a type of cryptographic technique in which different keys are used to encrypt and decrypt the data and information and are as shown in figure 1.2 [100].

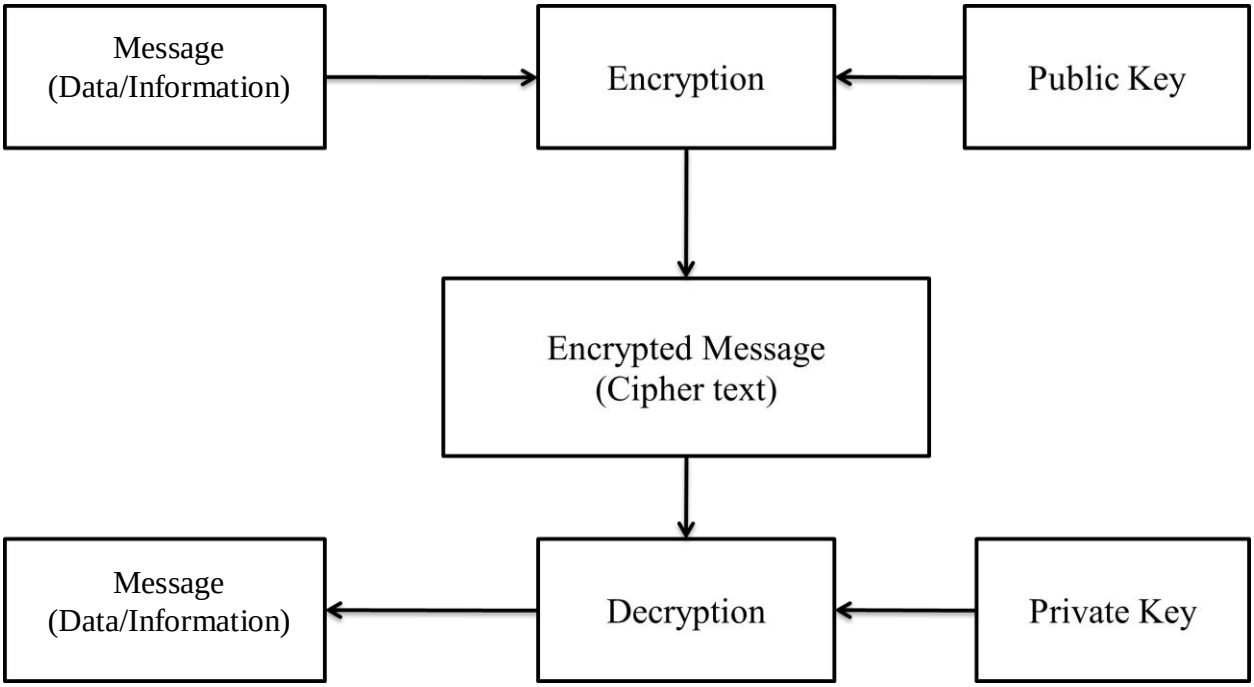


Figure 1.2: Block diagram defining asymmetric key cryptography

- **Symmetric Key Cryptography**: This is a type of cryptographic technique in which same key is used to encrypt and decrypt the data and information and are as shown in figure 1.3 [100].

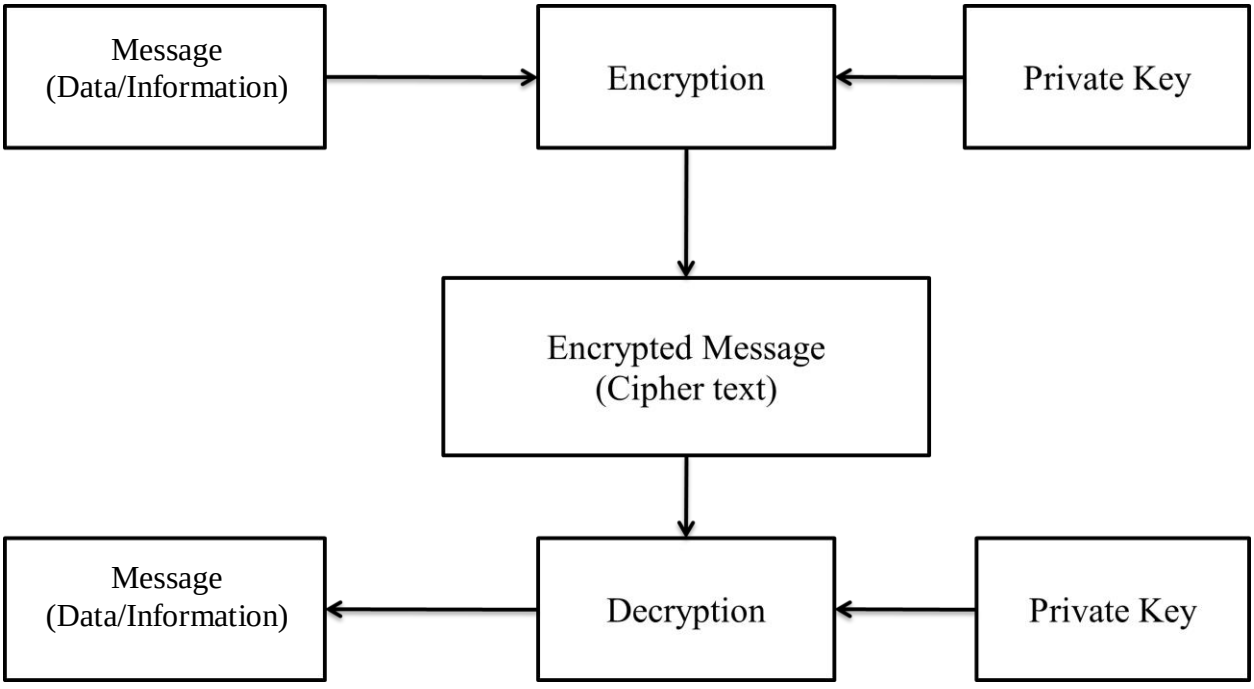


Figure 1.3: Block diagram defining symmetric key cryptography

Public Key can only be used for encryption whereas private key for both encryption and decryption.

- **Hash function**: This is a type of cryptographic technique in which the hash function is fed the secret message and it returns a fixed alphabetic string and this string is called as Hash value/ Digital fingerprint/ Checksum [100].

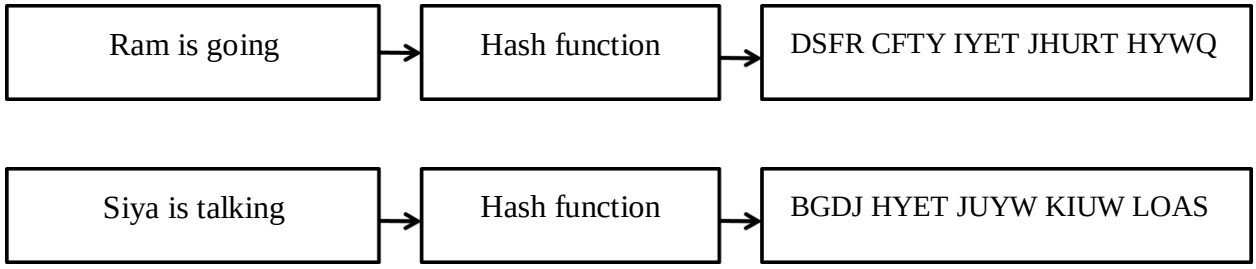


Figure 1.4: Block diagram defining basic data hiding approach (Hash function)

The figure 1.4 defines the hash value of any two data statements cannot be same and is unique for every statement therefore it is also known as digital fingerprints.

Information hiding: It is a powerful technique used for information protection in which the coder can encapsulate large number of elements to form a bigger entity rather the creating a large number to small entities which intern reduces the complexity of the system [100].

Watermarking: It is a technique in which an embedding code is added within any digital media like (image, audio, video etc) for the purpose of protecting authentication and maintaining of documents legality and to detect if there is any sort of tempering or alteration is done with the original document file [100].

Types of watermarking: The watermarking techniques are broadly classified in 3 main types which are described as:

- **Fragile watermarking**: The technique is used for checking for any unauthorized alteration in the given data. It becomes undetectable if there is any slight alteration in the file [100].
- **Semi-fragile watermarking**: This technique is used for checking any large alteration in the file. It becomes undetectable after any large alteration [100].
- **Robust watermarking**: This technique is used for unauthorized copy protection and is easily detectable [100].

Steganography: It refers to a technique in which one media is used as a cover for another media, the first media is known as the "cover" and the second media is known as "secret message". Thus, the process includes of hiding the secret message in the cover in such a way that no one is able to detect its presence in it as shown in figure 1.5. The condition for effective steganography is that the cover media should always be bigger than the secret message [99].

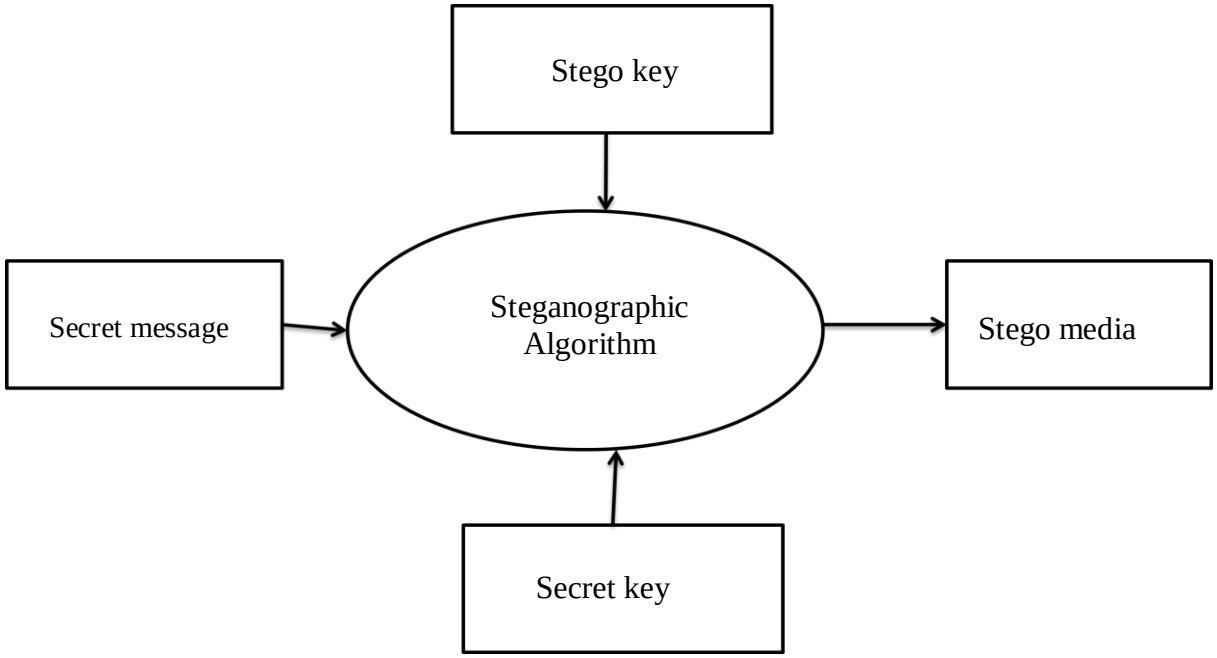


Figure 1.5: Block diagram defining basic concept of Steganography

Types of Steganography: The steganographic techniques are broadly classified in 2 types which are described as:

- **Linguistic Steganography**: This method is rather superficial as the changes done in the script is rather noticeable. This technique was used earlier but today is hardly in existence [99].
- **Technical Steganography**: This method is a bit advance compared to the linguistic method as hiding is done on the back end. The script hardly had gone under any type of significant difference. Hence, proving that this method is harder to detect then its previous counterpart and is rather preferred in various applications [99].

Types of Technical Steganography: The technical Steganography is broadly classified in 4 main types described as follows:

- **Image Steganography**: The steganographic technique which includes image as a cover for hiding secret message is known as image steganography [99].

- **Video Steganography**: The steganographic technique which includes video as a cover for hiding secret message is known as video steganography [99].
- **Audio Steganography**: The steganographic technique which includes audio as a cover for hiding secret message is known as audio steganography [99].
- **Text Steganography**: The steganographic technique which includes text as a cover for hiding secret message is known as text steganography [99].

The image steganography will be discussed and worked further in the thesis, following is an example shown in figure 1.6:

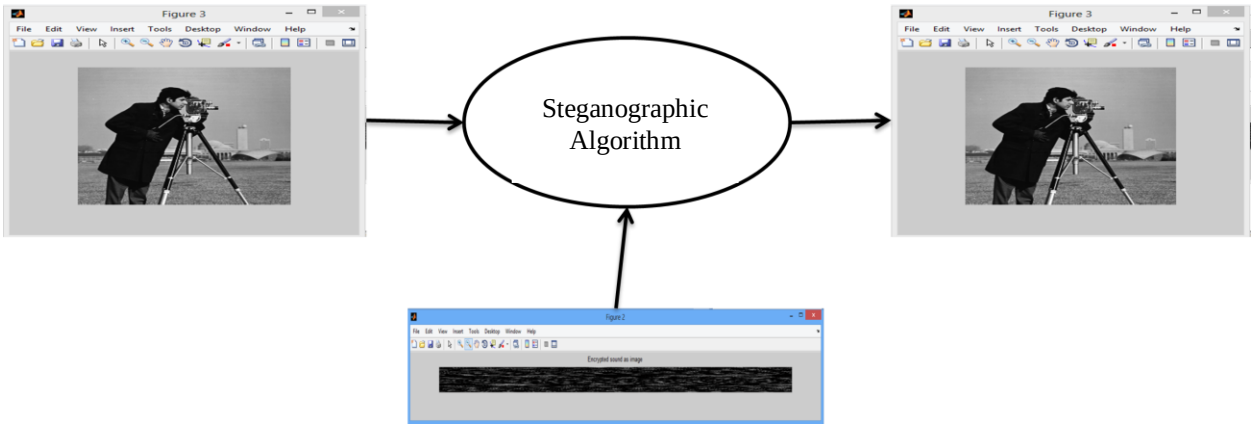


Figure 1.6: Worked example of image based steganography

It is a standard concept that "What You See Is, What You Get (WYSIWYG)" and follow when dealing or handling graphs and pictures or etc, but now a days it is no longer valid. This is not true as it is known to all that this doesn't holds always valid [19]. Images or graphics can be deceiving and could be much more then that one gets from his/her eyes. An image can convey information of much larger magnitude then tens of thousands of words. From centuries humans struggled to innovate any new type of method for confidentiality of important information. This demanded for an introduction and highlights and the briefly explanation of many of historical elements and various strikes of the method [23]. Through the presence of the steganography could be traced in the history literatures. Three of these techniques were precisely interconnected like cryptography, steganography and watermarking as shown in figure 1.7.

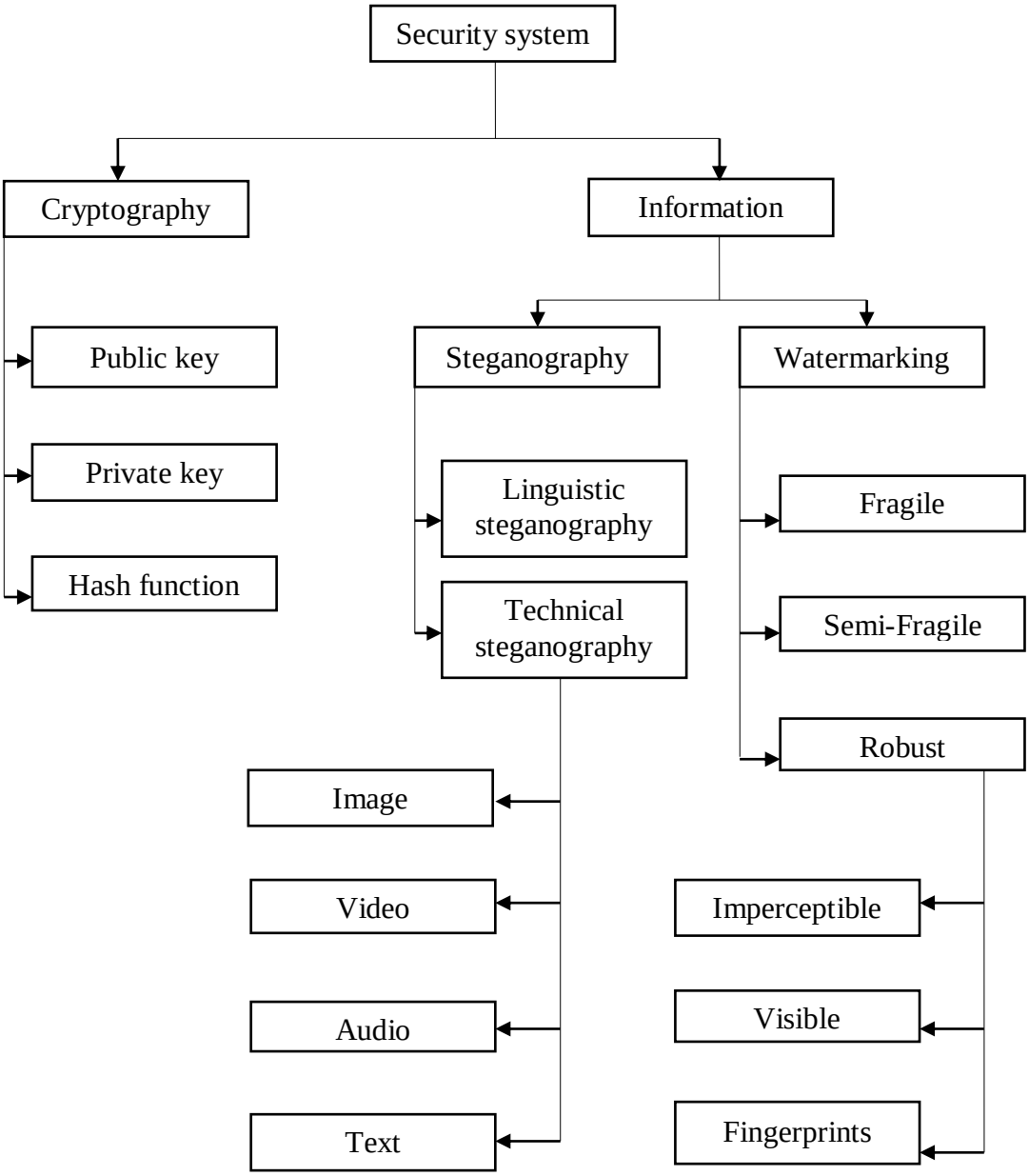


Figure 1.7: Evaluation based tree of security systems

Methodology	Steganographic measures	Watermarking measures	Encryption measures
Carrier	Media (digital)	Media (image/audio)	Textual (generally) Image (lesser)
Secret message	Secret key or payload	Water-marked	Cipher text
(I.D)Key	Non-vital	Non-vital	Vital
Input (minimum)	Atleast 2 or 1 self-embedding	Atleast 2 or 1 self - embedding	1
Identification	None Specific	Specific	None Specific
Validation	Full data	No data	Full data
Objective	Transmission of confidential information	Copyright preservention	Transmission of confidential information
Output (received)	Stego media	Watermarked file	Cipher text
Limitation	Capacity	None	None
Unauthorized breach	Steganalysis	Image processing	Cryptanalysis
Visibility	None	Only if permitted	Tough to distinguish
Failure	When detected	When removed/ replaced	When de-ciphered
Relationship with cover	Less then (<5%) Ideally (=1%)	Strong	None
Flexible	High	None	None
Introduced	Have traces in history	Recent	Recent

Table 1.1: Differentiating various types of data hiding techniques

The second and third are quite similar and hard to differentiate specially for the people from various other backgrounds; therefore, table 1.1 had been constructed to for detailed understanding and the presented work done over here is concerned with steganography of images (digital) also known as image steganographic technique.

Though the generalized model of any steganography could define for any number of arbitrary communication channels, but only the ones where the cover media is enriched with various multimedia objects, like an audio, an image, or a video file [25]. This is because of three causes:

- Firstly, the cover should be larger as comparison to size of the encrypted text. Ideally, the optimum embedding technique, doesn't allowed to be embedded anything greater than (>1%) then that of the size of cover [2].
- Secondly, indeterminacy within the cover is very important to be achieved for steganographic security. Larger the object better is it for indeterminacy, for example, the mathematical constant (π) which is a very highly precise and is unfavorable as a cover as unauthorized person will be able to detect their regular structure and separate the traces of embedded data/information [3].
- Thirdly, the hidden data which holds indeterminacy should be as small as possible. Audios and images are very much in abundance now a days within the communication environment that transmitting any such type of data can be undetectable [4].

In modern cryptography, it is very easily to assumable that Kerckhoffs' principle had been followed by digital steganography. This principle defined the steganographic algorithm for embedding secret information and then extracting it from within the cover should be public. Security can be achieved only by the help of secret keys sharing by the partners. However, the right interpretation of the principle in this case of steganography isn't quite easy, and the steganographer may be having additional degrees of freedom. Like, the choice of the cover had none of any direct effect in the standard cryptographic systems [9].

1.2 Nomenclature:

The word “cover image” would be utilized in the entire discussion to define the image produced to transmit the embedded secret message. It would be addressing an image consisting of hidden data, as “stego-image”. Thus, in either “steganalysis” or “attacks” referred to as seperate image processing with entirely different statistical analysis approaches but with same objective of breaking or attacking steganography algorithm [37].

1.3 History of steganography:

"Steganography" term was started from the antiquated greek word "steganos" which signified "secured" and "graphy" which implied "writing". It was employeed with various structures for a huge number of years. In mid fifth century Histaiacus shaved a slave's head, inked a message on his skull and the slave was dispatched with the message after his hair became back [1-4]. In Saudi Arabia at the King Abdulaziz City of science and innovation, a task was started to convert into english some antiquated Arabic original copies on mystery composing which are accepted to were composed 1200 years prior. Some of these original copies were found in Turkey and Germany [5]. Five hundred years back, the Italian mathematician Jerome Cardan re-evaluated a Chinese antiquated technique for mystery composing. The situation goes as takes after: a paper veil with gaps is shared among two gatherings, this cover is set over a clear paper and the sender composes his mystery message through the gaps at that point takes the veil off and fills the spaces so the message shows up as a harmless content as appeared in Figure 1.8. This strategy is credited to Cardan and is called Cardan Grille [4].

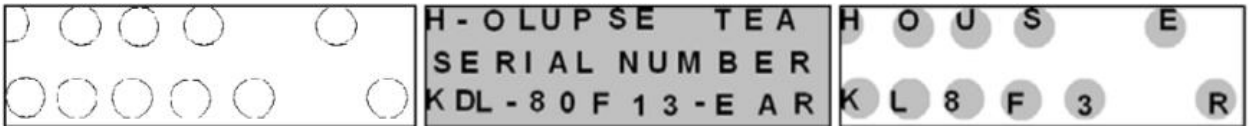


Figure 1.8: Cardin Grille: an illustration, of Grill pattern: (right) the hidden message, (middle) the cover and (left) the mask.

1.4 The digitization of Steganography:

As the beginning of another age the time of innovation it was found an exponential increment in computers, web and with the association of computerized flag preparing, data hypothesis and coding hypothesis, steganography went "advanced". Steganography had created an environment of corporate mindfulness that had given number of fascinating applications, and with its proceeds with improvement had ensured. The contemporary data concealing [9] is one of the hereditary strategy to show computerized steganography was shown by Kurak and McHugh [20], they recommended a method that was very like the installing system of 4 LSBs (minimum huge bits). These picture downsizing and the tainting are referred to today as picture steganography. It was believed that cybercrime can use it for their advantage. Therefore, an immediate response should be provided towards the undesirable uses of the steganography in the hands of terrorists followed by a report in USA TODAY1 [43]. Cyber chaos or “digital menace” proposed by the Lieutenant Colonel Timothy L. Thomas defined it would be difficult to control. Followed by this event Provos and Honeyman, started researching at the University of Michigan, and examined samples of more than three million images on internet from various popular websites finding any signs of steganography and they didn't find any secret messa [40]. Apart these fact that attributed various reason of that failure and this must be kept in mind that the steganography didn't occur in still images only. Embedded secret messages within any audio and video file are also possible. Existence of secret data and information within musical files, and their simpler format forms like Hyper Text Markup Language (HTML), Executable files (.EXE) and Extensible Markup Language (XML). This instance proved that USA TODAY’s claimed hadn't been based on any concrete fact, specially after this coming in light the writer who wrote the report resigned in two years after the editor's concluded that he was deceiving them during their investigation. They were centered around the report of steganography inside advanced pictures. The review on steganographic devices inside various media they had gotten measurable agent's point of view in light of that the per user was alluded to the utilizations of the steganography and the method close by inside were depicted in segments underneath. The real issue close by was centered around the spatial area procedures and the recurrence space systems and versatile methods inside advanced pictures. This could be seen in a significant number of the steganographic calculations described here and was recognized from steganalysis calculations and were more solid approach required to be resolved as enhanced and researched [43].

1.5 Application based on Steganography:

Now a days, Steganography has number of applications in various fields for communication, like copyright control for materials, increasing effectiveness of image searching through search engines and smart IDs distinctive ID's could be embedded within any image for analyzing present network traffic of any number of users, and the total number of embeddings [6]. Petitcolas portrayed few of the present day applications, of which one was utilized in Medical Imaging Systems where a classification is viewed as fundamental for patients i.e. test reports, x-beam comes about and their inscriptions, similar to, specialist, patient's close to home data and different particulars [17]. However, connect must be set up between the two. Along these lines, insertion of the patient's data in a picture can be demonstrated a pivotal safety measure and can furnish incredible help with thinking of answers for such issues. Steganography can fill in as a conceivable mean for giving and guaranteeing of confirmation that none other security apparatuses may guarantee. Miaou et.al. [27] proposed a LSB based installing system for keeping and keeping up records of electronic patients in light of bi-polar various base information stowing away. The variety between pixel estimation of a unique picture and its JPEG [4] form is thought to be a change base. Nirinjan and Li et.al. [30] examined covering of patient data inside advanced pictures. Roused by the steganography a Japanese firm Fujitsu3 began advancement of innovation of shroud information in a picture that was imperceptible to a human eye, yet must be uncovered with the assistance of a cell phone camera as showed underneath in figure 1.9. This technique took a not as much as a solitary second to embed data in around 12 bytes. Henceforth, the clients would have the capacity to use their mobiles to catch encoded any data. They took little charges for utilizing their deciphering programming. The base thought was the change of picture shading earlier the printing procedure to the Hue Saturation and Value segments (HSV) and afterward installing it in the Hue area which can't be recognized by human eye as they are not sensitive towards it. Mobile phone camera's are able to detect coded data and extract it. These application could find there utility in domains like-“doctor’s prescriptions, food wrappers, billboards, business cards and printed media such as magazines and pamphlets”, or can used in replacing barcodes where individual details were embedded in their images. There can be number of applications in various fields like safely sharing of any MNC's secret information, broadcasting of the TCP/IP packets [10]. The trust on the integrity of image had been ruined by the modern digital technology. Leading towards further researches on digital documentation and forensics. The example of this is Cheddad et.al. [37] proposel on security scheme that protected any scanned documentations from any type of forgery or any type of self embedding technique. This method didn'y pointed the forgery but also allowed legals and forensics experts for gain access on the un-forged documents even after being manipulated [19].

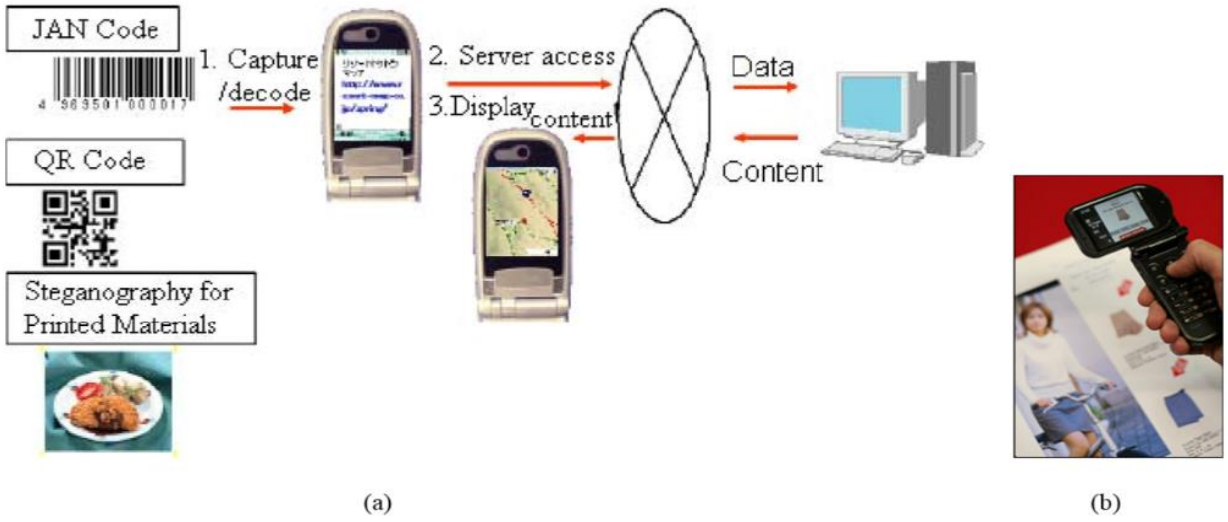


Figure 1.9: Some of steganographic applications employed by Fujitsu in- (a),(b)

1.6 Methodology:

In this section, an overview for a crucial steganographic technology using digital images is provided. There are number of formats present on the internet some of the popular are- Joint Photographic Experts Group (JPEG), Graphics Interchange Format (GIF), Portable Network Graphics (PNG), etc. Most of the approaches evolved were based on exploitation of the structures of the above formats with a few extensions in literatures they employed the Bitmap format (BMP) as it has simpler data structure [7]. The process of embedding is defined as follows:

Let C denote the cover carrier,

C^* be the Stego-image,

Let K represent an optional key,

Let M be the message,

E_m stands for embedding. Therefore:

$$E_m: C \oplus K \oplus M = C^*$$

1.7 Organisation of thesis:

In this thesis, the concept of image encryption and steganography had been discussed with the mention of various advancements and till date research reviews. The aim of this work is to add more security to the existing approaches and making the system more effective. The following is the outline and the contribution of each chapter in the thesis:

Chapter 1, briefly discusses about all the definitions of relevant concepts for understanding the basics of image steganography with its nomenclature, history, digitization, applications and methodology followed in the procedure.

Chapter 2, consists of work done of various researchers and their brief description based on the study conducted on the research work.

Chapter 3, contains all the research gaps recorded during the detailed study in previous chapter 1and 2, the objectives decided which are required to be achieved for optimum performance.

Chapter 4, record the work done during the thesis with the detailed procedure of the technique followed and all the upgrading done in it. It also consist of results of the work done with their descriptions.

Chapter 5, hold the comparison between initial and developed approach in addition with the concluding remarks and future scopes.

Chapter 2
LITERATURE REVIEW

2.1 Literature survey

This chapter consist of a brief description of some of the recognized recorded frameworks which are previously published works.

Mehdi Boroumand *et.al.* [1] demonstrated that express non-straight element maps combined with straightforward classifiers and enhanced the precision of current steganalysis indicators worked as two fold classifiers and also quantitative identifiers as payload regressors. The non-linear map acquired had little dependency on cover and low computational complexity this technique help to reduce error.

Bin Li *et.al*. [2] proposed an adjusted LBP form, called limit LBP (TLBP), to uncover the antiques caused by information installing. In this steganalytic conspire, the TLBP task was performed on leftover pictures which were gotten by utilizing an arrangement of high request subordinate filters to catch complex connections among pixels.

Yun-Te Lin *et.al.* [3] introduced an algorithm which exploited each three 10-bit mantissa as an embedded unit for concealment of k bits of a hidden message using a favorable base that provides the least pixel variations. This purpose, an expert encoder and decomposition scheme was suggested, that offered a high probability of transmission of $k + 1$ bits without causing an increase in pixel variation caused by message concealment.

Jishen Zeng [4] developed a generalized hybrid learning model of JPEG format steganalysis integrate the domain knowledge for the construction of an affluent steganalytic models. There were two main stages involved in the proposed framework. The initial stage was related to the convolution of phase and the quantization and truncation of phase of the affluent model. The successive stage was a gathered deep neural network consisting of multi deep subnets for which the modeled parameters were learned during the training procedures.

Alsharif Abuadbba *et.al.* [5] suggested that for maximum hiding, fast Walsh–Hadamard transformation was utilized for this transformation of signals were grouped and the signal having lowest distortion coefficients, was employed. The purpose of upgrading of security, the key was deployed in three-dimensional (3-D) faction of random coefficient for the concealment of the process. The resultant distortion was measured within all the stages.

Jan Camenisch *et.al.* [6] proposed an ideal functionality for non-committing encryption with locally generated, and therefore non-interactive, cipher texts. As a sanity check, they also provided a property based security notion that that proved to be equivalent to the universal composability framework that enables the modular design of cryptographic protocols by allowing arbitrary compositions of lower-level building blocks.

Tomas Denemark *et.al.* [7] defined a substitute kind of side information after examining a course of action of different JPEG photos of a comparable scene for applications when the sender does not approach a pre-cover. The additional JPEG pictures were used to choose the favored furthest point of embeddings changes to adjust the costs of changing individual DCT coefficients in a current embedding plan.

Kaibin Huang *et.al.* [8] introduced a dual-server PEKS (DS-PEKS) syntax to deal with this issue. There were front server and back server in their architecture and the keyword search test was done by the cooperation of two servers. Assumed that these two servers do not collude, the DS-PEKS scheme would be secure against offline inner keyword guessing attacks. They also proposed a new DS-PEKS construction based on the Cramer Shoup encryption, whose index and trapdoors are provably indistinguishable against chosen keyword attacks based on the IND-CCA2 security of the Cramer Shoup encryption without random oracle model.

Qinglei Kong *et.al.* [9] proposed a secure handover session key management scheme via mobile relay in networks. Specifically, to achieve forward and backward key separations, the session key shared between the on-board user equipment and the connected donor evolved nodes. It is first generated by the on-board user equipment and then securely distributed to the sub-nodes.

Mimi Ma *et.al.* [10] worked for development of a new well secured channel with a certificate-less searchable public key encryption standard with different keywords for host establishment. They also demonstrated a secure scheme of a random oracle model for two different types of portals, where one of the portal was granted the power over to choose any random public key on the exception of user's public key and the other portal was allowed to fetch the system master key.

F. Pelcastre *et.al.* [11] defined inverse halftoning algorithms based on Atomic Function and multi-layer perceptron neural network which provides gray scale images with PSNRs higher than 30dB independently of the method used to generate the halftone image, to obtain a more reliable approach for

the representation of the provided image with lesser noise interference and a higher distinct data representation.

Zhiniang Peng *et.al.* [12] introduced circulant rainbow with shorter private key and higher marking efficiency. In circulant rainbow, they brought turning relations into parts of rainbow private key to accelerate the marking methodology and diminish the private key size. They painstakingly pick security parameters so that there circulant rainbow is secure against every known assault.

Indranil Ghosh Ray *et.al.* [13] provided an efficient simple to actualize open key based accessible encryption conspire for string seek which were adaptively secure and does not require any record. They had given solid confirmation of the versatile security of their plan against fair however inquisitive server.

Shunquan Tan *et.al.* [14] proposed a technique based upon pixel decimation, which was a particular form for image downsampling which was based upon a theoretical analysis and an empirical evaluation, which clearly confirmed that these methods damaged the synchronization of the embedding changes during steganography and helped in improving the efficiency of embedding change and its probability estimation.

Weixuan Tang *et.al.* [15] introduced a programmed steganographic contortion learning structure utilizing a generative ill-disposed system, which is made out of a steganographic generative sub-organize and a steganalytic discriminative subnetwork. Through then again preparing these two oppositional subnetworks, there proposed system can naturally pick up implanting change probabilities for each pixel in a given spatial cover picture.

Yuqi Wang *et.al.* [16] gave a model by studying the recent quantum public-key encryption. This model made an explicit stipulations on the generation, distribution, authentication, and usage of the secret keys, thus forms a black-box operation for continuous observation of the keys and avoid any danger or threat to repeat based on the record of the previously stored data.

Xiaogang Wang *et.al.* [17] defined an encryption standard in which an image would be encrypted in two phases, one being the input phase and other being the conjugate plane phase. They presented it in a divergent wave spherical field which when compared with its counterpart used planar and symmetrical key. It demonstrated a significant difference in an continuous changing of positions of an optical element which was allowed for encryption, resulting in a decryption keys which was varied from that of encryption keys (or their conjugates) of variable sizes.

Junxiang Wang *et.al.* [18] proposed about the development rate of distortion model, the problem of HS-based multiple embedding is formulated as the one of rate and distortion optimization. Two key propositions were then derived to facilitate the fast computation of distortion due to multiple shifting and narrow down the solution space, respectively.

Zhiwei Wang [19] defined a character based information collection convention for the brilliant lattice. They didn't just anticipated an unapproved perusing but also find protected the breaking down or any other likewise. Ensuring effective measures against accidental blunders and perniciously adjusted messages.

Zhuo Wei *et.al.* [20] proposed a novel and secure key-sharing framework named progressive character based mark key sharing. It comprised of a key age, key transmission, and key administration. To sort the authorized personal from any unauthentic intruder and hence providing the system with adequate safety measures for protection of system information from getting in wrong hands.

Yan Xu *et.al.* [21] worked for the expansion of the studies of their technique and came up with a an advanced version know as variable approached technique, based on best of their knowledge. It was considered as a first work that had been achieved in diversifying the system security. The technique developed for taking three types of authorization for providing dynamical protection of the privacy of the data owners. Thus, been the best furthest approach for the strengthens of the security and the privacy in a 5G network.

Jian Ye *et.al.* [22] introduced an elective way to deal with steganalysis of computerized pictures in light of convolutional neural system. It appeared to have the ability and capacity to well reproduce and improve these key strides in a unified structure. Thus, gaining various leveled portrayals specifically from crude pictures.

Weiming Zhang *et.al.* [23] suggested a technique including non additive distortion steganography and defined the joint distortion in pixel block. To reduce the complexity and to minimize the joint distortion, they came up with a design of code for decomposing the joint distortion. The distortion of the individual pixels were so that, the message could be efficiently embed with syndrome trellis codes.

Huishuai Zhang *et.al.* [24] defined a standard for all models studied, the key capacity region was established by designing a unified achievable strategy to achieve the cut-set outer bounds. They also studied the problem of generating more than two keys and characterize its key capacity region. Where all the cellular terminals were required to generate independent keys with the base station.

Hang Zhou *et.al.* [25] introduced an attacking method on steganography, which could not only detect the stego-images but can also extract the hidden messages. This technique was based on image synthesis for steganographic encryption detection by pixel detection of given image. Thus, efficiently extracting the secret message embed within the image pixels elements.

Wenbo Zhou *et.al.* [26] proposed a novel cost reassignment manage, which is connected to not one but rather a bunch of existing bending capacities. They found that the costs allowed on a few pixels by a few steganographic strategies might be altogether different despite the fact that these techniques display close security levels. They called such pixels "disputable pixel".

Cong Zuo *et.al.* [27] introduced a variation of accessible open key encryption named concealed token accessible open key encryption with two new security properties: token namelessness and one-token-per-trapdoor. With the previous security idea, the customer can acquire the pursuit token from the information proprietor without uncovering any data about the basic watchword.

A. S. Brandao *et.al.* [28] proposed a technique for more effective and secure data transmission by employing steganography. This technique required the involvement of least significant bit for inserting images into digital images. The detection and decryption of the information was done with the help of artificial neural networks.

Rongmao Chen *et.al.* [29] defined a cryptographic encryption security was quite useful for the protection of the data and information present online or in the cloud storage. It was discovered that the online and cloud storage data was under threat with a special type of attack known as the inside keyword guessing attack. The dealing with this threat they came up with a new technique known as dual server.

Rongmao Chen *et.al.* [30] suggested a new and better version of the system known as server aided public key encryption standard. In this technique, for the generation of the keyword cipher text/trapdoor the administrator needed to bring a third party in the trust circle this third party is called keyword server. It helped in the processing by maintaining security, by employing authenticating protocols and protects the system against offline threat. They further introduced an universal transformation from converting any technique to a secure technique by employing it.

Shengda Chen *et.al.* [31] presented an improvement in approach for programmed identification and manufactured portion confinement of protest based fashioned video encoded with cutting edge structures.

The approach begins with a casing control locator. A programmed calculation was also proposed to distinguish protest construct video imitation situated in light of the casing control finder.
Tomas Denemark *et.al.* [32] proposed that classifiers built from detectors trained for countering steganograhic parameters that could provide most accuracy for a channel. As it was observed that JPEG images based steganographic algorithms was best for detected by histogram of the noise residuals by incoperating best information about the channel.

Jaroslaw Duda [33] introduced a novel technique for producing outwardly engaging two-dimensional (2D). Thus, standardized identifications that take after important pictures to human spectators. The innovation of 2D standardized tags, at present overwhelmed by speedy reaction codes, was broadly embraced in numerous applications. It included item, archivements, administration and general advertising.

Debiao He *et.al*. [34] studied another unknown versatile client confirmation convention that used the self certified open key cryptography for multi-server structures. Rather than the current conventions, brings about lower calculation and correspondence costs. By contrasting and two of the most recent conventions, the calculation and the correspondence expenses of their convention were no less than 74.93% and 37.43% lower than them, individually.

Fangjun Huang *et.al*. [35] proposed a new and effective technique for encryption domain. In this technique, the pixels within a plainer image were divided further in sub blocks of size ($p \times q$). Then, with the help of pseudorandom codes combining with the information a new set of encrypted text was produced the pixels within the encryption sub block with similar key stream byte.

Fengyong Li *et.al.* [36] introduced a technique that employed higher ordered joint featured and clustered ensemble. It employed a (250 D) featured calculation with a higher ordered joint matrix with discrete cosine transformation coefficient of JPEG images, which indicated the dependency of the image content.

Klimis Ntalianis *et.al.* [37] defined a strong authenticating mechanism for semantic segments, chaotic encryptions, and data hiding. Taking for instance, assumed that any user X wanted to remotely authenticate with initially was automatic segment, by employing a head and body detector. Further, biometric signal of X was encrypted in cipher. Thus, the encrypted cipher signal would be inserted to the most valid wavelet coefficient and employed it in qualified significant wavelet trees .

R. Tavares *et.al.* [38] introduced the concept of LSB Word Hunt. It was an excellent LSB technique based upon the idea of the word hunt puzzle. The major objective of the LSB based word hunt was to minimize

the expected count of transformation per pixel. This purpose of insuring high security and low detection for the LSB based encrypted file for prevention of the disguise from getting blown.
Vahid Sedighi *et.al.* [39] proposed an unique approach based upon a calculated multiple variant. Gaussian cover image modeled for sufficient and simplified enough for deriving a content. The adaptive Least Significant Bit (LSB) matching yet complex enough for capturing of the non stationary characteristics of any image.

Hengchuan Tan *et.al.* [40] introduced a safe and verified key administration convention to defend the weaknesses of the system. The conspire disseminates storehouse containing the ties of the substance's character and its relating open key to every vehicle and street side unit. Thus, certificate trades and certificate denial records were killed.

Weixuan Tang *et.al.* [41] defined a technique known as clustering modification directions for color components. The basic operation of this technique was to transform various color component of the same pixel position towards a increment or decrement consistently. To apply this technique, they break down an image in various sub parts in which segments of hidden message bits were embedded.

Weixuan Tang *et.al.* [42] suggested a technique of assigning variable weights to various pixels during feature extraction. The pixels corresponding to higher weight had larger data embedded in them and thus more significant compared to those having low weights and lower embedded data within them. By following this technique, they were able to concentrate their attention on the high significant regions instead of whole image.

Xianyi Chen *et.al.* [43] introduced an approach that calculated the differences among pixel pairs and proved that the histogram of variable values would be smoothed due to the presence of stego-noises. They calculated the (DHCF) Difference Histogram Characteristic Function and deduced that the moment of DHCFs (DHCFM) will be diminished after stego bits were hidden in the image. Accordingly, they computed the DHCFMs as the discriminative features.

Guanshuo Xu *et.al.* [44] proposed novel design that considers learning of steganalysis. In the point by point design, total estimations of components in the element maps were produced from the first convolutional layer. They encouraged and enhance measurable demonstrating in the consequent layers.

Jiang Yu *et.al.* [45] introduced a novel plan for spatial steganalysis in view of complexity of residuals. Subsequent to choosing complex pieces from an uncompressed picture by a fluctation work, the residuals were computed from the chosen squares and the entire picture in the wake of applying differing filters.

Weiming Zhang *et.al*. [46] defined a novel structure for the view of reversible picture change. Not the same as all past encryption based systems, in which the figure writings may pull in the documentation of the inquisitive cloud, based structure enables the client to change the substance of unique picture into the substance of another objective picture with a similar size.

Jung Hee Cheon *et.al*. [47] introduced a system which employed a PKE for encryption of messages and were carried by SHE after decryption. To achieve an efficient decryption a new hybrid technique was formed by combining without any complication like earlier with SHE. Moreover, if was multiplicative by nature, the proposed technique not had any difficulty evaluating the polynomial.

Remi Cogrannewe *et.al.* [48] proposed to employee a measurable model of such a gathering and supplant the larger part voting principle with a probability proportion test. This enabled them to prepare the group to ensure wanted measurable properties, for example, the false-alert likelihood and the location control, while saving the high identification precision of unique gathering classifier.

Bingwen Feng *et.al.* [49] defined an image based steganographic approach which was aimed in reducing the embedded distortion. Initially the text pattern, rotation, compliment were extracted from within a binary image. When the weighted sum changed while flipping a pixel it then measures the corresponding distortion of that pixel.

Linjie Guo *et.al.* [50] introduced a technique focused on making embedded modification proportional to coefficient of variation within a digital image This new technique was considered to be substantial and considered usage of discrete cosine transform coefficients for direct currents, zero and non-zero for alternating currents as covers.

Vojtech Holub *et.al.* [51] defined a novel concept of rundown capacities for steganalysis of JPEG pictures. The features were worked as first orchestrate bits of knowledge of quantized uproar residuals got from the decompressed JPEG picture using 64 bits of the discrete cosine change (DCT).

Bin Li *et.al.* [52] proposed an approach that can hamper the associations among embeddings changes in order to diminish the risk of distinguishing proof by steganalysis. It used a novel framework, called gathering modification orientation, in light of the supposition that while embeddings modifications in seriously completed regions were locally. The heading towards a comparative course, the steganographic security might be gained ground.

Sha Ma *et.al.* [53] defined the authentication technique by employing for the enhancement of users privacy. They also defined new policies in accordance with various updating techniques along with providing security and authentication at the same time by random model of oracle. Thus, making it harder for the intruder to penetrate through the security system of the device.

Mohamed M. E. A. Mahmoud *et.al.* [54] introduced different motivations that necessitate revoking certificates in smart grid. They also identified the applications that could be secured and thus needed certificate revocation. Then, they explained existing certificate revocation schemes and define several metrics to assess them. Based on the assessment, they identified the applications that were proper for each scheme and discuss how the schemes could be modified to fully satisfy the requirements of their potential applications.

Tung-Tso Tsai *et.al.* [55] defined a tending to the denial issue and its first revocable certificateless open key encryption. They defined the new linguistic structure and security ideas and proposed a solid conspire for the advance protection of the system in case of system breached by the intruder for making it the primary target of the system security by putting a pause on all existing operations.

Kuo-Chen Wu *et.al.* [56] proposed a technique for the extraction of hidden message. This approach offered various advantages. Firstly, this technique offered higher embedded capacity directly proportional to the size of the image. Secondly, this technique was hard to trace and decrypt. Thirdly, the recovery of hidden message was easy if technique was known.

Linjie Guo *et.al.* [57] introduced the concept of uniform embedding distortion. The function of most recent addition to the class of distortion functions that is known to be present in JPEG based steganography. Using this technique they were able to come up with a minimum distorted by spreading the embedded information with uniformly quantized discrete cosine transform coefficients of various values.

Jan Kodovsky *et.al.* [58] proposed the concept of evaluation for what happens if the image was down-sampled before being embedded. They came up with various parameters effecting the result like- resizing, choice of kernel, scaling factor, down-sampling pixel grid alignment. They recorded various phenomena's that appeared during steganographic applications.

Bin Li *et.al.* [59] suggested the concept of evaluation of cost assigning in 2 parts finding the priority and specify the cost distribution. Their analysis illustrated the cost distribution determined the rate of change of elements the cover scheme was immune towards various steganographic models.

MA Xiaojing *et.al.* [60] introduced a JPEG compatibility steganalysis calculation that assessed the installing rate in light of the contrast between the stego picture and its recompression based anticipated cover picture. Specifically, pressure curios and installing changes were recognized in light of the abundancy of pixel esteem changes. This was done autonomous of the implanting positions, consequently was successful for both substance non-versatile and content versatile steganography.

Hasen Nicanfar *et.al.* [61] proposed an effective technique that adjusts authorized. This adapts a smart meter present in home area network with help of smart servers with self guidence by employing initially set passwords. Thus, therefore decreased the number of subsequent stages within a the secure remote password protocol.

Thanh Hai Thai *et.al.* [62] defined a factual model of quantized discrete cosine change coefficients. It was depended on a numerical structure of concentrate the picture handling. The pipeline of an average advanced camera as opposed to fitting experimental information with an assortment of mainstream models.

Keren Wang *et.al.* [63] proposed a technique for finding respective motional vector's present in video steganography. Initially the LSB of motional vector's were modified. The outcome of the embedded operation on the sum of absolute difference was defined. This allowed them on focusing on the variation between the combined and local optimum afterwards of the addition/subtraction operations upon the motional values.

Bo Dai *et.al.* [64] defined that the security helplessness exists just in the channel while the duplex phase shift keying channel could impede these assaults. In this way, the idea of open key cryptography was acquainted into the framework with efficiently utilized. These two orthogonal channels for both open key dispersion and encoded information transmission.

Gokhan Gul *et.al.* [65] introduced that visually impaired steganalysis of JPEG pictures. They were tended to by demonstrating the relationships among the discrete cosine transformation coefficients utilizing k-variate. The gauges built by methods for Markov arbitrary field factions. The thinking of utilizing high k-variate together with inner circles for picture steganalysis was clarified through an established identification issue.

Vojtech Holub *et.al.* [66] defined an option factual portrayal as opposed to framing the co-event framework. They anticipated neighboring remaining examples onto an arrangement of arbitrary vectors and took the first arrange measurement (histogram) of the projections as the component. At the point,

when various residuals were utilized, this portrayal was known as the projection spatial rich model (PSRM).

Ayman Ibaida *et.al.* [67] proposed a wavelet based steganography system which had been presented with consolidated encryption and scrambling strategy to ensure understanding confidential information. The technique permits system security flag to shroud the comparing persistent confidential information and other physiological data in this manner ensuring the reconciliation amongst the security and the rest operations.

Fengyong Li *et.al.* [68] defined a JPEG steganalytic plot in light of high-dimensional highlights and Bayesian outfit classifier. The proposed conspire utilizes 15700 measurement highlights computed from the co-event lattices of discrete cosine transformation coefficients and coefficient contrasts This showed the intra-piece and between square conditions of picture pixel content.

Chuan Qin *et.al.* [69] proposed a technique of reversable steganography for similar image identification/matching in which initially a reference pixel. It was chosen in accordance with the distributed characteristics further employing image imprinting technique. In which the based differential equations were casted for generation of odd images with same geometry and structure and information as above/cover.

Jie Ren Shih *et.al.* [70] introduced an execution of novel based concept of two posted quantum public key cryptographic systems. Initial step in securing a machine-to-machine system employing strong assisted quantum public key cryptographic systems. Although the primitive quantum public key cryptographic systems techniques were unsupportive for machine-to-machine but the current version was made compaitable with it all in terms of maintenance, deployment and management.

Leif Uhsadel *et.al.* [71] defined a concept based on public key encryption. This application played a vital role as was attractive for teaching/learning purposes but due to its structural complexity. It hardened the applicability of microcontroller based programs. Although a simpler smaller version was developed for application based microcontroller but was indeed shorthand in providing equal results as the original one.

Yun Cao *et.al.* [72] suggested the adoption of few new motion vectors as during research that came across some unfavorable selection rules which could be violated by encoding the motion vectors in an unorthodox method. They came up with a new set of selection rules which could detect the features of steganalysis.

Yu-Chi Chen *et.al.* [73] worked to cryptanalyze the Hu–Tzeng scheme and show that it is not cheating immune. They also outline and helped in the improvement to overcome the problems. The overall combined effort help in optimising the all round performance and also came forward with an updated version of the scheme.

Lionel Fillatre [74] proposed a technique for the recognition of secret data within LSB based image. It was based on adaptive co-variance matrices which kept the probability distribution. The independence of the unknown parameters of image embedded which indeed ensured the high detection ration of secret message.

Jessica Fridrich *et.al.* [75] introduced a structure on three steganographic calculations intended to conceal messages in pictures spoke to in the spatial area: HUGO, edge-versatile calculation by Luoetal, and ideally coded ternary 1 installing. Every calculation, they connected a straight forward sub-display determination method. To expand the discovery exactness per demonstrate dimensionality and show how the identification soaks with expanding many-sided quality of the rich model.

Wien Hong *et.al.* [76] proposed an innovative technique of embedding secret information based upon pixel pair matching. The basic concept under this technique was using of pixel pairs as reference coordinates and investigate the image by pixel pairs. Once any detected the system detects the pattern and thus the secret message.

Fangjun Huang *et.al.* [77] introduced an innovative channel selection rules for joint photographic experts group (JPEG) format steganography that could be helpful in detection of discrete cosine transform coefficients which can cause distortions for secret message embedding. Thus, playing a crucial role in unmasking, identifying and extraction of the secret message.

Jan Kodovsky *et.al.* [78] defined an option and surely understood machine learning instrument troupe classifier. It actualized as irregular woodlands—and contented that they were in a perfect world suited for steganalysis. Troupe classifier scale significantly more good w.r.t. the quantity of preparing cases and the element dimensionality with execution com illustration to the substantially more perplexing and defending the system security.

Che Wei Lee *et.al.* [79] suggested an identification technique based on secret dispense with self healing capability for grayscale image for PNG format. The shared values were mapped and embedded near the maxima (255) resulting in better disguised and an overall effective encryption.

Hafiz Malik *et.al.* [80] introduced a steganographic technique for quantization index modulation. The technique was constructed keeping in mind to detect the randomness in test images for differentiating between cover and stego image. The results displayed showed the once without embedding as without irregularities whereas the embedded once with irregularities thus separating the embedded once from the normal once.

Shunquan Tan *et.al.* [81] defined an image steganography based on LSB matching. They introduced a pulse disruption on the long exponential edge of the plotted histogram between the absolute difference of the pixel pairs. Thus, concluding the observation of the B-spline fitting technique.

Ching-Nung Yang *et.al*. [82] suggested the technique for mastering the shortcoming of the Rey's method. It was as designed so that even for low rank matrices the security can be confirmed and the secret message can't be extracted from its shadow image thus preventing it from giving access to unauthorized personal.

Tomas Filler *et.al.* [83] evolved a technique to limit added substance bending in steganography with general installing task. Letting each conceivable incentive for each stego component be appointed to a scalar communicating the contortion of an implanting change done by supplanting the cover component by this esteem. The aggregate contortion was thought to be an entirety of per component bends.

Chung-Li Hou *et.al.* [84] proposed a technique with lesser disruption in detection and extraction. The method worked on all type of embedded files despite of there size of embedding be smaller or larger. The extraction was much simpler in this version of the technique compared to its previous counterparts.

Xiangyang Luo *et.al.* [85] suggested the steganalysis strategy which meant to get the measurable of mystery existing in sight and sound transporters. The key worry for outlining a visually impaired steganalysis calculation were to be determination of measurement highlights. The probability density function minute and characteristic function minute. They were two regular sorts of measurement includes generally utilized as a part of visually impaired steganalysis.

Weiqi Luo *et.al.* [86] proposed a compelling technique for recognition of the quantization table. From the encoded advanced pictures which were initially put away as JPEG design. In the light of the late improvement works about JPEG pressure blunder examination and after that exhibited a quantitative strategy. The dependably gauge the length of spatial modifications in grayscale JPEG stegos utilizing information fitting innovation.

Hung-Min Sun *et.al.* [87] defined the work displayed in a hostile to legal steganography strategy that could be installed and extricated the messages from pictures. Feature of abusing modification course and versatile techniques .They utilized the module tasks and assessed the senstive idea of a human visual framework.

Wei-Jen Wang *et.al.* [88] introduced the classification of information concealing techniques into four non-covering bunches as per their reversibility and yield positions. They presented the points of interest of the delegate strategies, outline the highlights of the agent strategies, and think about the execution of the delegate techniques utilizing crest motion to commotion proportion, limit of mystery information, and bit rate.

Gokhan Gul *et.al.* [89] defined the concept on relationship between the steganographic model of an image and the row and column. The values of that image matrix is linear by nature. They demonstrated using a weiner filter by decomposing singular value transformation. This approach was most superior compared to all its previous.

Jing Ming Guo *et.al.* [90] introduced the concept of a embedding factor which help to define the amount or quantity of embedding that can be done within a JPEG image .The embeddings were such in nature that the made small alterations in the format without affecting its quality and causing any suspicion. They also defined a quantization table for it which helped in embedding of secret message.

Guo-Shiang Lin *et.al*. [91] defined a continuous loop system that repeatedly explore for a better set of pixel coefficients. To maximize the extend of steganographic effect that could be applied without causing any suspicion. The loop system was continuous and consist of an anti-steganographic tester for increasing maximum embedding with least cost affected.

Weiqi Luo *et.al.* [92] suggested the LSB coordinating returned to picture steganography and edge versatile plan. It could choose the installing locales as indicated by the span of mystery message and the distinction between two back to back pixels in the cover picture. To bring down installing rates, just more honed edge areas were utilized while keeping the other smoother locales as they were. At the point, when the installing rate expanded, more edge areas could be discharged adaptively for information covering up by changing couple of parameters.

Tomas Pevny *et.al.* [93] proposed a technique for identifying the steganographic scheme that had been employed for the embedding of data within. In this technique a low magnitude independent stego-signal is applied to the media and detect the desirable results. This technique had been successful on LSB scheme.

Anindya Sarkar *et.al.* [94] defined employing technique for matrix embedding repeat accumulate technique. It was an excellent union of matrix hiding technique conjugated with repeated accumulated coding to minimize error. A major pro of this technique was the greater likelihood ratio of repeat accumulation decoders accounting many to one mapping for matrix embedding based values.

Jun Zhang *et.al.* [95] proposed an outstanding detector used for detecting and extracting the noise based residuals. The discrete cosine transformation domain and were vital for predicting LSB scheme. This technique increased the overall operational efficiency and improved greatly the processing ability of the image effectively.

2.2 Observations based on literature survey:

A observations regarding the existing model were made and following statements were derived:

- The model was relatively simpler in structure with less complexity
- No pre-encryption present.
- No suitable cover selection process present.
- Less security levels present.
- Once the image gets detected the entire approach is trashed.

Chapter 3

Statement of problems based on identified research gaps and objectives

3.1 Introduction:

The research gaps deals with the loop holes present within the present state of the investigation or experimentation results and outcomes. The purpose of the research gaps is to narrow down the gaps of undefined expressions and the combine the previous results and the present ones for making the nature or response of the system more compatible. Thus, the results would be more organized defined and well explained considered to be more satisfying and resourceful.

3.2 Gaps:

Having stated that LSB is an good steganographic technique it faces the following challenges:

- It is a very simple technique and faces ease of extraction.
- The cover image must be casual and based on some characters that it should be only recognizable to the sender and the receiver.
- It must varying colors, (preferable colored) to be divergent "noisy", in order to hide the little bit but significant changes can't be detected. Otherwise a plane having uniform shade would be quite noticeable with or without any keen vision.
- The other problem is with the file size, which involves the choosing of the format. Unusually big files exchanged between two parties, is most likely to arise suspicion.
- JPEG or any lossy format cannot be employed because of their lossy, compressions and it will be more prone to looses of important information.

3.3 Objectives:

The main focus of efforts are to optimize the performance of the existing system. To achieve the goals that have been set up following objectives which will be achieved for enhancing and securing the system performance:

- To add few layer in the present data embedding system for further filtering and refinement of results to be achieved.
- To add a pre-encrypting stage before the embedment of the secret message/data.
- To introduce a decision box for appointment of the best cover setup for the secret message/data (keeping in mind all the significant parameters like - data capacity, divergence/noise present in image, size, format like JPEG, PNG etc).
- To add a disguise to the transmission (i.e. sending number of images of similar format pattern and appearance).

So, that only the desirable party/person which will be knowing about the distinctive parameter or clue should only be able to obtain, decrypt and read the message. These objectives will help us to get one step closer in building better secure system then the already present version .

Chapter 4

Results and Discussion

4.1 Work done:

Learning based steganalysis methods consider the detection of hidden message as a classification problem in which regardless of whether the test picture has a shrouded mystery message will be resolved. The extraction of discriminative features is the key point for steganalysis problems. Many previous steganalysis methods calculated sensitive features by analyzing two influences introduced by the hidden messages. Some methods extracted features by calculating the smoothness of the histogram of pixel values. Others calculated the discriminative features by analyzing the correlations between the adjacent pixels. The demonstration of the difference histogram calculated from the pixels in an image that became smoother after a secret message is embedded by LSB matching. This change is utilized to extract features for hidden message detection.

As previous approaches described were not up to date in terms of standards for the present day security requirements but it was quite helpful in defining some of the flaws where it can be improved. It have been provided with suitable advancements which saw were need for raising its standards described with following advances:

- Providing of encryption of date previously before initiation of its embedding process.
- Decision and selection of suitable covers which provide high attributes of colors for raising the noise of the image so as to disguise or hide the little bit significant changes done in the cover doesn't draw any attention.
- Employing lossless formats for embedding of secret message.
- Embedding data according to the cover chosen or vice versa, so that the embedded data doesn't reaches detectable levels.
- Always transmitting cover images in group of simple images for not drawing any suspicion.

Image Format	JPEG	PNG	BMP
Digital Image	33.05	28.4	33.03
Natural Image	32.94	27.75	33.09

Table 4.1: PSNR of digital image and natural image of various image formats

Image Format	Losses	Size/Capacity
TIFF	Lossless	Very large
JPEG	Lossy	Large
PNG	Lossless	Large
BMP	Lossless	Large
GIF	Lossless	Small
Raw image	Lossy	Large

Table 4.2: Comparison between various image formats in terms of losses and size/capacity

The instructive tables above (table 4.1 and table 4.2) describe the various characteristic parameters of the various image formats which assists us in deciding a suitable cover for the secret message.
From the given formats in the upper table 4.1

- the digital format is best suited as it has greater scope of embedding as compare to the natural format

From the given formats in the table 4.2

- The TIFF format is the best because of its lossless nature and high resolution pixel values, but it was rejected as the size of the file with TIFF based format is very large and cause large disruption due to transmission and channel noise plus and file of that large size will attract suspecion. So, PNG/BMP formats were chosen.

4.2 Feature extraction:

The Learning Based Steganalysis (LBS) method considered the detection of the secret message as a classification problem within which whether or not the test image had any hidden secret message would be determined. The extraction of the discriminative features were the key point for the steganalysis problem. Many of the previous steganalysis methods were calculated using sensitive features and by analyzing the two influenced the hidden messages. Some of the methods extracted the features by calculating the smoothness of the histogram and of its corresponding pixel values. Others calculated based on the discriminative features and by analyzing the correlations between the adjacent pixels. The demonstrated difference histogram calculated from the pixels in an image that became smoother after a secret message was embedded by LSB matching. This change was utilized for extract features for the cover image for secret message detection.

4.3 LSB matching:

LSB matching embeds the secret message bits by slightly modifying the pixel values in an image. The LSB of the pixel value equals the stego bit, no change will be made to this pixel. Otherwise, the pixel will be changed by adding or subtracting 1 at random. Denote as the grayscale magnitude of pixel at the position in image I, where x=(i,j)∈{0,…,n_1-1}×{0,…,n_2-1} and n_1, n_2 are dimensions of the image (I) in the vertical and horizontal directions, respectively. Denote the cover image and the stego one as and , respectively. The secret bit is embedded as

$$I_S(x) = I_C(x) + \xi(x) \tag{1}$$

where $\xi(x)$ represents the secret bit at the position x $P\{\xi(x) = 1\} = P\{\xi(x) = -1\} = \rho/4$, $P\{\xi(x) = 0\} = 1 - \rho/2$, and $\rho \in (0,1]$ is the embedding rate.

Change of pixel difference:

Denote an image pixel pair as (x_0,x_1). The two pixels do not need to be neighboring ones. Then, the difference between the two pixels (x_0,x_1) can be calculated:

$$d(x_0, x_1) = I(x_0) - I(x_1) \tag{2}$$

After message embedding, the difference will be changed accordingly. With the differences before and after the embedding denoted by $d_c(x_0,x_1)$ and $d_s(x_0,x_1)$, respectively, the change of $d(x_0,x_1)$ can be denoted as:

$$\begin{aligned} C_d(x_0, x_1) &= d_s(x_0, x_1) - d_c(x_0, x_1) \\ &= I_s(x_0) - I_s(x_1) - I_c(x_0) + I_c(x_1) \\ &\quad \xi(x_0) - \xi(x_1) \end{aligned} \tag{3}$$

The $\xi(x_0)$ and $\xi(x_1)$ can be assumed to be independent of each other. Further, according to the symmetry of $\xi(x)$, the following can be obtained:

$$\begin{cases} P\{C_d = 2\} = P\{C_d = -2\} = \rho^2/16 & (4) \\ P\{C_d = 1\} = P\{C_d = -1\} = \rho/2 - \rho^2/4 & (5) \end{cases}$$

Change of difference histogram:

First, a difference matrix D can be constructed as:

$$\begin{aligned} D(i,j) &= D_{\Delta x, \Delta y}(i,j) \\ &= d((i,j),(i+\Delta x, j+\Delta y)) \\ &= I(i,j) - I(i+\Delta x, j+\Delta y) \end{aligned} \tag{6}$$

where (i) and (j) indicate the positions of the difference values, and denote the distance parameters in the vertical and horizontal directions, respectively. Then, the histogram of D is calculated as:

(7)

$$h_D[n] = \frac{1}{|D|}\sum_{i,j} \emptyset\{D(i,j) = n\}$$

$$n = -255 \dots 0 \dots 255$$

where $\emptyset\{D(i,j) = n\} = 1$ if $D(i,j)$ equals n; otherwise, $\emptyset\{D(i,j) = n\} = 0$. According to (4) and (5) equations:

$$\begin{cases} E(h_{Ds}) = h_{Dc} * f, \\ f = \{\frac{\rho}{16}, \frac{\rho}{2} - \frac{\rho^2}{4}, 1 + \frac{3\rho^2}{8} - \rho, \frac{\rho}{2} - \frac{\rho^2}{4}, \frac{\rho^2}{16}\} \end{cases} \quad (8)$$

where (*) denotes the convolution; the D_c and D_s denote the difference matrices that are computed with the original image and the stego version,respectively; and h_{Ds} and h_{Dc} denote the normalized histograms of D_c and D_s respectively.

DHCFM :

In this method, we measure the change of difference distribution in the frequency domain is measured. Given a serial of real number:

$$g = g(n); n = 0 \dots \dots \dots N-1$$

we perform discrete Fourier transform (DFT) as follows:

$$G[k] = (DFT\ g)(k) = \sum_{n=0}^{N-1} g[n]\, e^{\frac{-2\pi jnk}{N}}$$

$$k = 0 \dots \dots \dots N-1 \quad (9)$$

Similar to[4], the DFT on (g) is the characteristic function (CF) of g. Similarly, we denote the CFs of h_{Ds},h_{Dc} and f as H_{Ds},H_{Dc} and F, respectively, i.e.,

$$H_{Dc}[k] = (DFT\ h_{Dc})(k)$$

$$H_{Ds}[k] = (DFT\ h_{Ds})(k)$$

$$F[k] = (DFT\ f)(k) \quad (10)$$

where H_{Dc} and H_{Ds} are the characteristic functions of difference histogram (DHCF). Then, according to Equation (8),we obtain:

$$H_{Ds}[k] = H_{Dc}[k]F[k] \quad (11)$$

The smoothing in the spatial domain indicated the decrease of the energy at the high frequency part in the frequency domain. We measure this type of change by the DHCFM as:

$$\text{DHCFM} = \sum_{k=0}^{N/2-1} \text{k}|\text{H}_\text{D}[\text{k}]| \quad (12)$$

After the messageis hidden, DHCFM will be decreased, i.e.: $\text{DHCFM}_s \leq \text{DHCFM}_c$ (13)

Proof of Formula(13): We denote $n\epsilon\{-M \dots\dots\dots M\}$, $M = (N-1)/2$. Then, we can rewrite the DFT on $f[n]$ as:

$$F[k] = (DFT\, f)(k) \sum_{n=\_M}^{M} f[n]\, e^{-2j\pi kn} \tag{14}$$

$$\sum_{n=-M}^{-1} f[n]\, e^{-2j\pi kn} + f[0] + \sum_{n=1}^{M} f[n]\, e^{-2j\pi kn}$$

where f[n] is a real even sequence. Thus, we have:

$$\sum_{n=-M}^{-1} f[n]\, e^{-2j\pi kn} = \sum_{n=1}^{M} f[n]\, e^{-2j\pi kn} \tag{15}$$

Thus, Equation (14) can be rewritten as:

$$= \sum_{n=1}^{M} f[n]\, e^{2j\pi kn} + f[0] + \sum_{n=1}^{M} f[n]\, e^{-2j\pi kn} \tag{16}$$

$$= f[0] + \sum_{n=1}^{M} f[n]\, e^{-2j\pi kn} + f[n] e^{2j\pi kn}$$

$$= f[0] + \sum_{n=1}^{M} 2f[n]\cos(2k\pi n)$$

$$\leq f[0] + \sum_{n=1}^{M} 2f[n] = 1$$

Finally,

$$DHCFM_S = \sum_{k=0}^{M} k|H_{Ds}[k]|$$

$$= \sum_{k=0}^{M} k|H_{Dc}[k] + F[k]|$$

$$\leq \sum_{k=0}^{M} k|H_{Dc}[k]|$$

$$\leq DHCFM_C$$

4.4 Calibration:

All types of images are being used as covers. Accordingly, the features that are extracted from images vary significantly, which could conceal the change of features caused by message bits. The designed calibration method to decrease the influence of image content on the features to alleviate the influence of the image content. Given an image, a calibrating image is produced through an average filter as:

(17)

$$I'(x) = \frac{1}{|N'(x)|} \sum_{N'(x)} I(x')$$

where $N'(x)$ denotes the deleted neighborhood of (x), and $|N(x)|$ denotesthe number of pixels in $N'(x)$. The DHCFM feature that is calculated from the image is denoted by DHCFM(I), and the DHCFM features are computed from both (I) and (I'). Then, the feature is calibrated as:

$$DHCFM(I') = \frac{DHCFM(I) - DHCFM(I')}{DHCFM(I)} \quad (18)$$

4.5 Conclusion:

A steganalysis method has been proposed to reveal the existence of stego messages hidden by LSB matching. Unlike most existing methods, the differences between pixels that have a great distance from each other are utilized to extract discriminative features for steganalysis. It demonstrates that the hidden messages smoothen the difference histogram. The DHCFMs are calculated as the discriminative features. The features are further calibrated and utilized to construct SVM classifiers. The detection performances exhibit the adequacy of the proposed strategy.

4.6 Results:

Figure 4.1:Original image

The figure 4.1 is the original image without any kind of embedding of any secret message. It is very important part for the steganographic process as poor selection of any cover image can lead to suspicion and detection of the secret message turning the whole process to trash (preferable a moderate size image with high color ratio is ideal for the process).

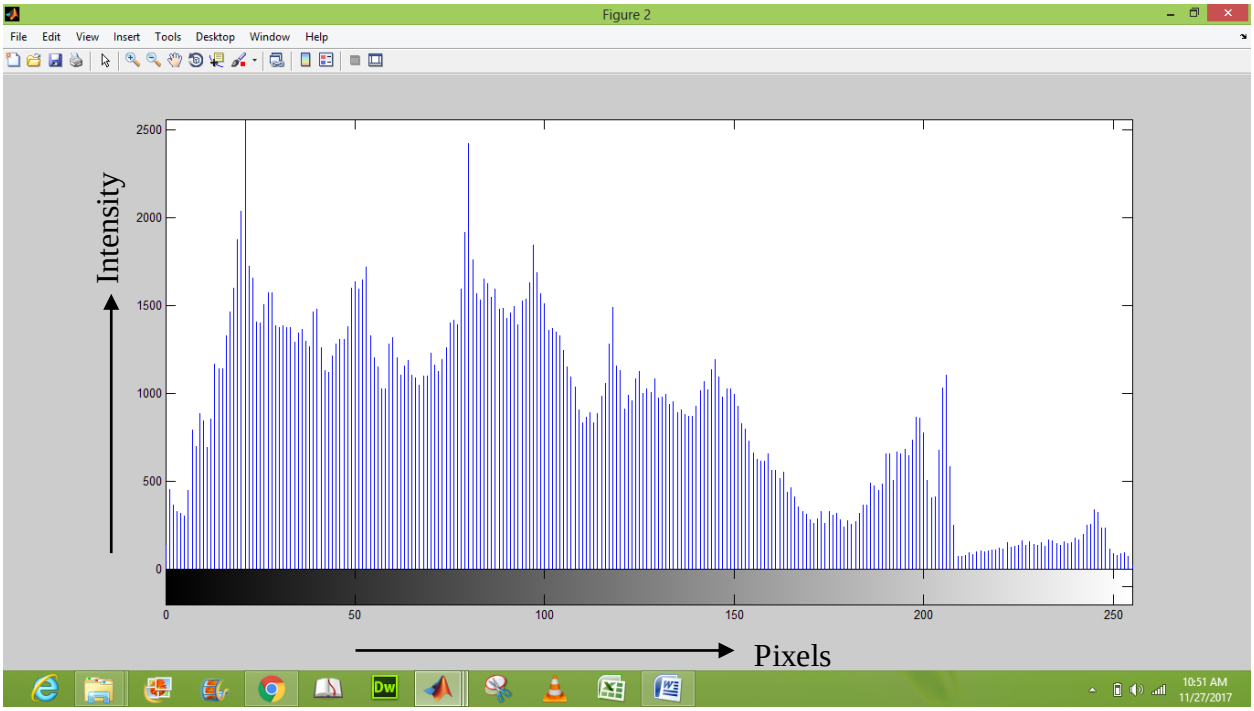


Figure 4.2:Histogram of original image

The figure 4.2 depicts the histogram of the original image with its corresponding characteristic curve of pixel to intensity values. This is the original curve of the image it can be seen it has high difference values between peak to pit values.

Figure 4.3: Secret message embedded image (stego-image)

The figure 4.3 depicts the stego-image or the embedded secret message image, this is the final processed version of the original image as told earlier the image choose should be of moderate size and high color ratio so that the minor or little change done in the image during embedding could be cover with already existing colored noise of the image. Causing least or none of suspicion to it.

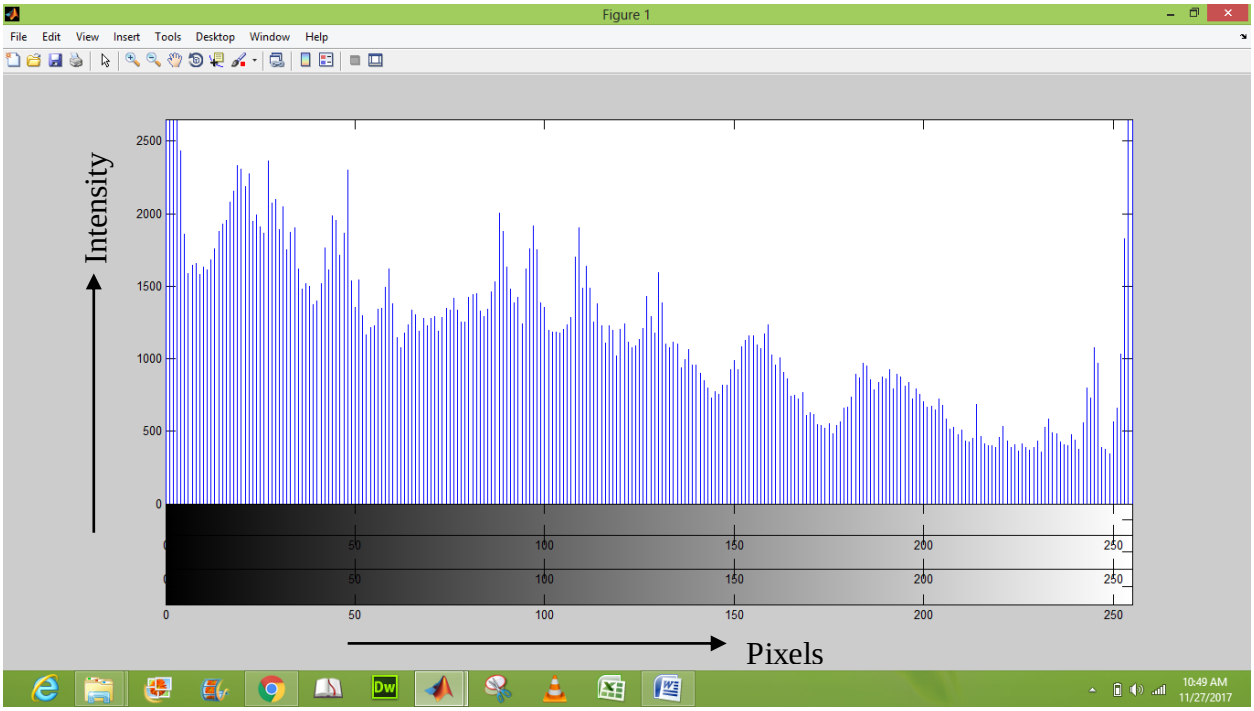


Figure 4.4: Histogram of stego-image

The above figure 4.4 depicts the histogram of the embedded stego-image. Here the histogram is not a single variant histogram. The histogram presented in the figure 4.5 is a convolution of all the three colors of the basic spectrum of light (red, green and blue variants respectively). Need of this convoluted form is because the data embedding is done uniformly in all the three planes. If any one variant will be missing, it won't make any sense on the retrieval of the information because some part which rests in the missing variant won't be there. As seen above the peak to pit value difference is lesser in this histogram as compared to the previous one in figure 4.4. This is because the embedding is done within these peak to pit values to minimize any type of detectable change.

Chapter 5

Comparison, Concluding Remarks and Future Scope

5.1 Comparison:

Image steganography is the craftsmanship and study of hiding a message in a picture by altering picture pixels as well as recurrence coefficients. The most vital necessity in steganography is imperceptibility. Accordingly, different steganographic strategies endeavor to insert messages in an indistinct way with the goal that the subsequent stego is like its relating spread picture outwardly and factually. LSB substitution is the most straight forward steganographic technique. Nonetheless, it brings some asymmetry antiques into stegos, and along these lines it is effortlessly recognized utilizing some steganalytic techniques, for example, Chi-squared assault [11], normal/solitary gathering investigation [10] and test combine examination. LSB coordinating was then prepared to evacuate asymmetry ancient rarities presented by LSB substitution by means of arbitrarily adding ±1 to pixel values. Contrasted with LSB substitution, LSB coordinating enhances undetect capacity significantly. In this manner, some run of the mill strategies, for example, LSB coordinating returned to and PVD [3], were additionally included later. The above techniques can be viewed as non-versatile steganography, which implies that the modified pixels after information covering up would be arbitrarily spread over the entire picture. Nonetheless, it is demonstrated that pixels situated in textural districts have much preferred concealing properties over those in smooth locales, and this reality is utilized as a part of some versatile steganography. In the versatile steganographic procedures, every pixel inside the cover picture is firstly doled out an inserting cost. A mutilation work is then defined in view of the implanting costs, and finally the subsequent stego is given by means of limiting the twisting capacity utilizing some coding systems, for example, STCs (syndrome trellis codes). Contrasted with the current non-versatile innovation, versatile techniques as a rule accomplish considerably more grounded security. A portion of the versatile steganographic procedures are as per the following:

- In EA the mystery message is inserted into the edge locales as indicated by the distinction between two neighboring pixels.

- WOW [8], is a strategy, which can adaptively install mystery message into cover picture as indicated by textural unpredictability.

- HUGO BD [24], is the substance based versatile steganography strategy for spatial pictures which can around safeguard the joint measurement of contrasts between up to four neighboring pixels in four distinct ways.

- S-UNIWARD [9], the mutilation between the cover and stego picture is figured as a whole of relative changes of wavelet coefficients speaking to the two pictures and afterward the pixel is then implanted with the mystery message.

- ASO [22], it based on oracle used to figure the delectability map, and utilize the Kodovsky's outfit classifiers [39]. Both cover image and sender's database appropriations amid the implanting procedure, which enhances the security.

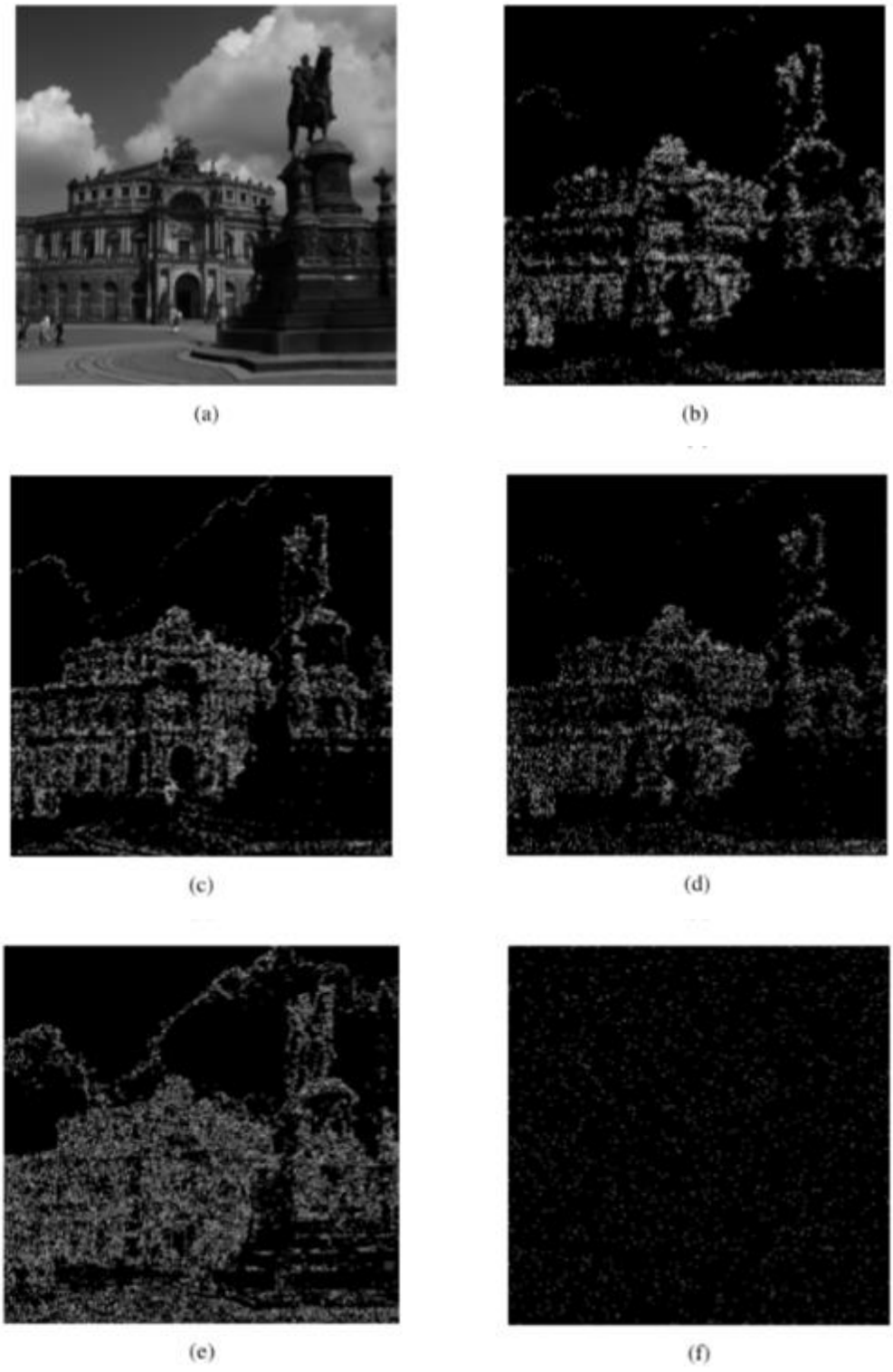


Figure 5.1 Delineation of cover picture and the comparing modifications utilizing WOW, HUGO BD, S-UNIWARD, EA, and LSB coordinating (0.3bpp). (a) Cover Image. (b) WOW. (c) HUGO BD. (d) S-UNIWARD. (e) EA. (f) LSB matching.

5.1.1 Versatile Steganography Restriction Analysis:

In this section, common embedding properties are demonstrated of versatile steganography, and afterward the breaking down the confinement of versatile steganography in view of the installing probabilities.

5.1.1.1 Embedding property of Steganography:

Figure 5.1 demonstrates a case of a cover picture and the relating modification outline five average steganographic strategies, including WOW, HUGO BD, S-UNIWARD, EA, and LSB coordinating, with the same inserting rate of 0.30 bpp. It can be seen that the areas of the modifications change for various versatile techniques. The purpose behind the distinctions is that different versatile steganography would apply various installing methodologies. For LSB coordinating, the modified pixels were haphazardly situated in the entire picture. For the EA strategy, sharp edge areas were firstly considered for information covering up. While the other three techniques (i.e., WOW, HUGO BD, and S-UNIWARD) were composed under the structure of limiting a defined twisting capacity, as outlined in Figure 5.3. In this system, each pixel was first allocated an installing cost, which speaks to how much contortion it takes to change a specific pixel, at that point a twisting capacity was defined in view of the inserting costs, and finally some coding procedures, for example, STCs, were utilized to limit the mutilation work and acquire the subsequent picture stegos. It should be noted that one of the fundamental contrasts between steganographic strategies under such a structure was the plan of the inserting cost. For example, in ASO [22], the implanting cost was the total of all perceptibility costs acquired from various FLD classifiers. In HUGO [17], the installing cost was figured as the separation between the SPAM highlight separately removed from the cover and the stego. HUGO BD [24] was an enhanced variant of HUGO and its inserting cost thinks about the collaborations of installing inside a nearby neighborhood. In WOW [8], the installing cost was computed as the conglomeration of the progressions of various directional high-pass wavelet filters. For S-UNIWARD [9], the implanting cost was ascertained as the total of the relative changes of the coefficients in the wavelet filter banks and so on.

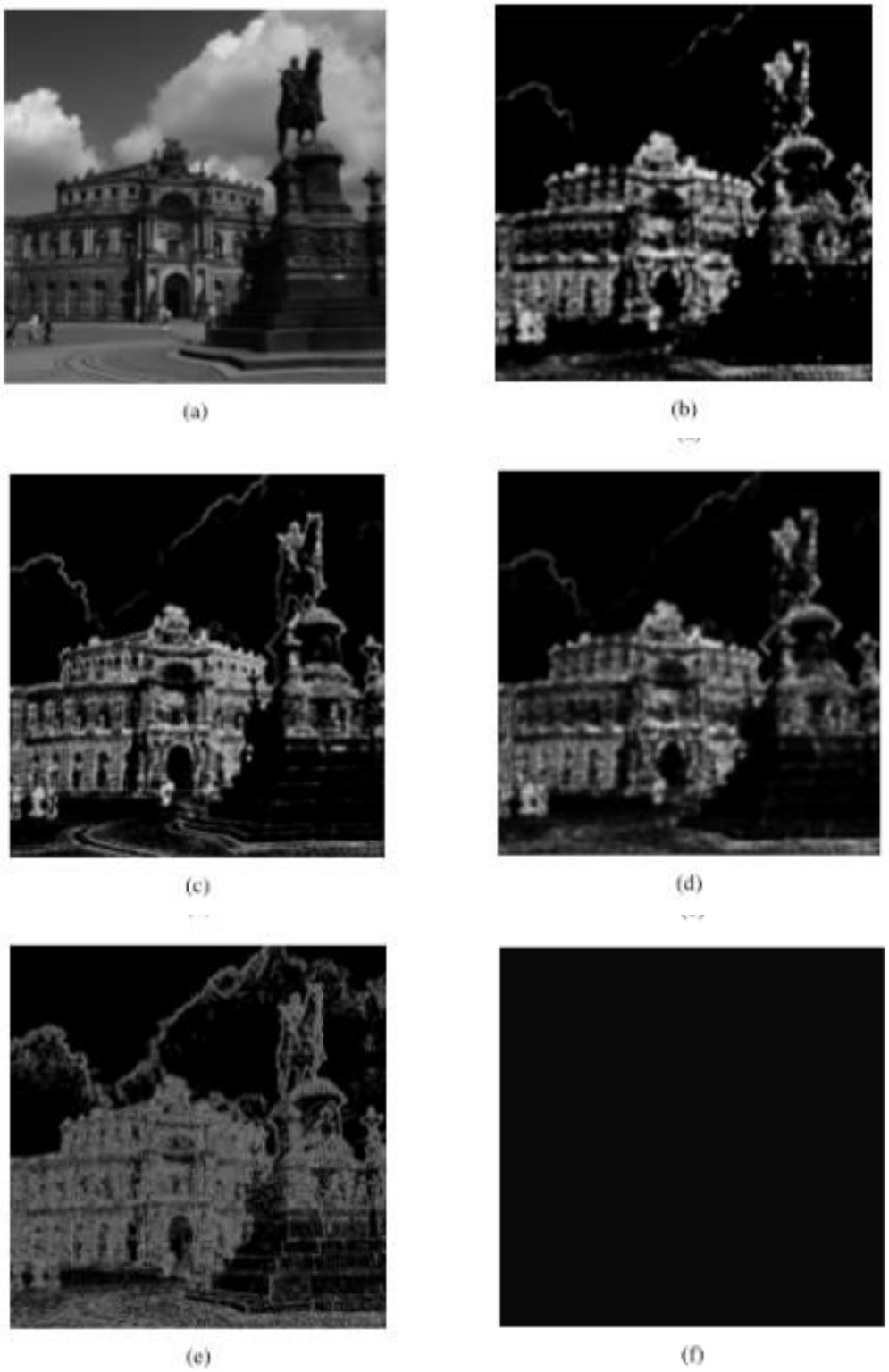


Figure 5.2 Outline of cover picture and the comparing inserting probabilities/likelihoods with WOW, HUGO BD, S-UNIWARD, EA, and LSB coordinating (0.30 bpp). (a) Cover Image. (b) WOW. (c) HUGO BD. (d) S-UNIWARD. (e) EA. (f) LSB matching.

Figure 5.2 (b)- (e) indicate likelihood maps relating to Figure 5.1 (b)- (e). It should be further noted that the scale installs probabilities in a scope of [0,1] to a scope of [0,255] for show purposes, and Figure 5.2 (e) was somewhat dim because of the installing likelihood of every pixel being near zero. It would be ideal if looked at the modifications in Figure 5.1 and the relating inserting probabilities in Figure 5.2 beneath. It was discovered that in spite of the fact that the modifications were diverse for various versatile steganography, the regular characteristic they shared were that the modification outline fundamentally were the same as its corresponding likelihood maps. The accompanying subsection, examine the connection between the modification guide and likelihood guide, and attempt to uncover the normal confinement of versatile steganography.

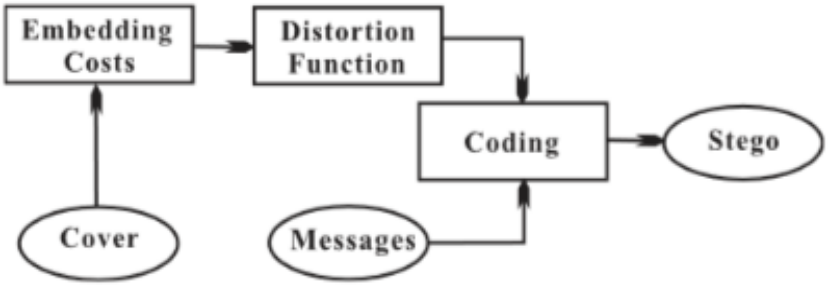


Figure 5.3 Versatile steganography technique in view of the structure of limiting the distortion function.

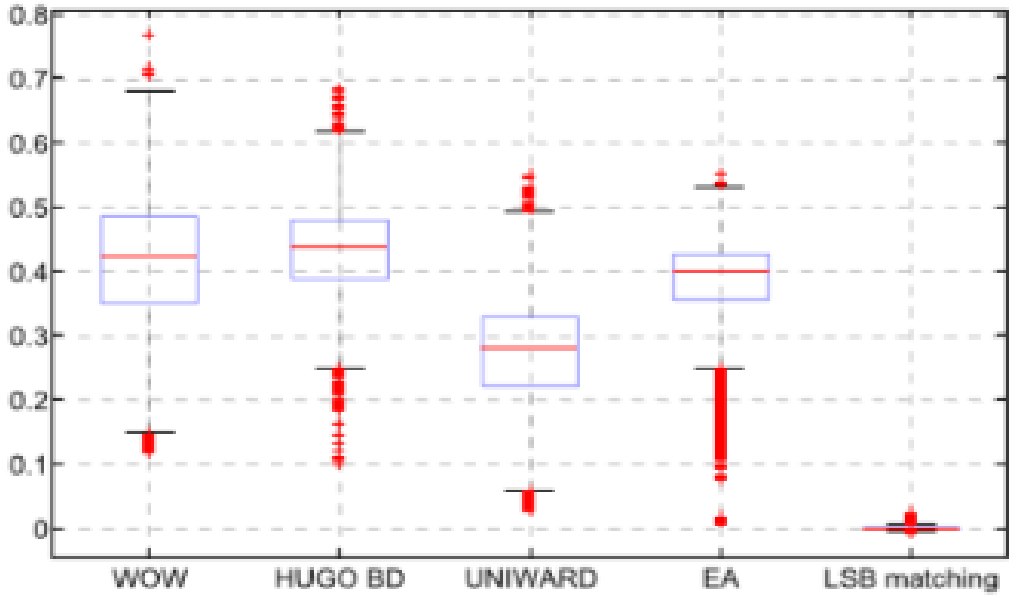


Figure 5.4 Box plot of the correlation coefficients for different steganography [98]

5.1.1.2 Constraint Analysis Based on Embedding Probabilities:

As portrayed in Section [5.1.1.1], a likelihood map may assist us with estimating the areas of modified pixels in versatile steganography. In this examination, the relationship was figured between the evaluated implanting likelihood and the genuine modification after information covering up. For any picture under a given inserting rate to be assessed, the installing likelihood delineate firstly evaluated from the picture, which was then put away in a vector. Essentially, the modification outline (set the comparing component as 0 if the pixel has not been modified after information stowing away and as 1 generally) is put away in a vector with same length. At last, the relationship coefficients can be computed between the two vectors. It was normal that the higher the relationship coefficients, the more exact the modified areas can be assessed. On the off chance that the connection coefficients achieves the most extreme value 1, the ground truth implanting probabilities would be equivalent to the modification, which implies that it can precisely find the greater part of the modification for this situation. Figure 5.4 demonstrates the boxplot of the connection coefficients assessed on 10,000 cover pictures from BOSS base [29] for various steganographic strategies with the same installing rate of 0.30 bpp. From Figure 5.4, it was watched that the connection coefficients of versatile techniques were substantially bigger than those of the non-versatile strategy (e.g., LSB coordinating), whose relationship coefficients were around zero. In view of the above examination, it was found that inserting prob-capacities can furnish with valuable data for assessing the areas of potentially modified pixels after information concealing utilizing versatile steganography, which was useful in steganalysis. In light of these data leaked in versatile steganography.

5.2 Exploratory Results:

Four average versatile steganographic techniques, i.e., WOW [8], HUGO BD [24], S-UNIWARD [9], and EA [27], were incorporated. To assess the execution of identifying versatile steganography for a given installing rate, in the preparation organize, an estimation of implanting probabilities of 5,000 haphazardly chose cover pictures and their relating stegos individually were made by the inserting rate, and after that got their versatile SRM highlights. The subsequent highlights were then used to prepare an outfit classifier [14]. In the testing stage, it played out similar tasks for any testing picture to acquire versatile component, which was then nourished into the relating classifier, as it was in most existing steganalytic writing, without considering the obscure inserting payload issues. The identification execution was quantified utilizing the testing mistake, which was the normal of the false alert rate and the missed discovery rate. Also, the reference arrangement of the versatile steganalysis and is considered in the analyses. From any cover picture and its comparing stego, in getting the areas of modifications. Pixel weights were set as "1" if the comparing pixel esteems were changed after information stowing away and were something else "0". It would be ideal if taken note of that in the reference framework, weight delineate cover and its relating stego was the same. The reference framework was required to give an

upper bound on location execution since it just consider the modified pixels (i.e., pixels with weight 1) for highlight extraction. It would be ideal if taken note of that the areas of the modified pixels were not accessible in genuine applications. Be that as it may, the reference framework can manage us to outlining an appropriate versatile plan and demonstrate the potential for the versatile steganalytic technique. As the inserting probabilities can be gotten in two distinct cases, individually.

Embedding Rate	**SRM required/ effectiveness (in %)**	**Method with maximum likelihood (in %)**	**Innovated Method (in %)**	**Reference Method (in %)**
0.05 bpp	45.44	38.98	36.48	35.68
0.10 bpp	40.66	33.24	30.71	30.32
0.20 bpp	31.68	26.30	24.11	23.85
0.30 bpp	26.69	22.13	19.59	19.15
0.40 bpp	20.92	18.81	16.69	16.12
0.50 bpp	16.90	15.85	14.20	14.11

Table 5.1 Detection error for Innovated vs WOW using optimal simulator

Embedding Rate	**SRM required/ effectiveness (in %)**	**Method with maximum likelihood (in %)**	**Innovated Method (in %)**	**Reference Method (in %)**
0.05 bpp	43.42	37.43	35.72	35.20
0.10 bpp	35.92	32.93	30.98	30.26
0.20 bpp	28.20	26.05	23.76	22.79
0.30 bpp	22.39	21.06	19.80	18.97
0.40 bpp	18.24	17.32	16.85	15.98
0.50 bpp	14.60	14.01	13.58	12.56

Table 5.2 Detection error for Innovated vs HUGO BD using optimal simulator

Embedding Rate	SRM required/ effectiveness (in %)	Method with maximum likelihood (in %)	Innovated Method (in %)	Reference Method (in %)
0.05 bpp	45.44	43.60	42.39	42.31
0.10 bpp	40.66	39.10	36.92	36.88
0.20 bpp	31.68	31.50	29.72	28.76
0.30 bpp	26.69	25.25	24.12	23.54
0.40 bpp	20.92	20.64	20.04	19.34
0.50 bpp	16.90	16.50	16.19	15.70

Table 5.3 Detection error for Innovated vs S-UNIWARD using optimal simulator

5.2.1 Getting Embedding Probabilities by means of Optimal Simulator:

For the situation where the versatile steganographic strategy was composed. The system of limiting the added substance contortion work and the implanting strategy was known as inserting probabilities. It can be precisely evaluated by the ideal test system. For relative investigations, the first non-versatile steganalysis SRM [6], past work [28], the technique [23] and the proposed strategy were incorporated into the tests. Three versatile strategies, i.e., WOW [8], HUGO BD [24], S-UNIWARD [9], planned under an indistinguishable system from that delineated in Figure 5.3 were assessed. For every steganography, six distinctive implanting rates going from 0.05 bpp to 0.5 bpp were tried. In the past techniques [28], the execution were influenced by a parameter P, and the identification mistake with the best parameter P was given in all trials. The identification comes about are appeared in Tables 5.1, 5.2, and 5.3 individually. From Tables 5.1, 5.2 and 5.3 it can be seen that both past technique [28] and the proposed strategy outflank the first SRM much of the time, particularly for WOW and HUGO BD with implanting rates lower than 0.20 bpp. Taking WOW for instance, the upgrades in the past technique [28] and the proposed strategy were as high as 6.46% and 8.70%, separately, when the implanting rate is 0.05 bpp. Among the three steganalytic techniques, the proposed strategy works best in all cases. Contrasted with the first SRM, were acquired 6.09%, 3.77%, and 1.74% normal upgrades for WOW, HUGO BD, and S-UNIWARD, separately. Contrasted with the past work [28], an additionally acquiring 1.76%, 1.52%, and 1.00% normal changes for WOW, HUGO BD, and S-UNIWARD, individually. The strategy [23] were analyzed under the same steganalytic highlights (i.e., horizontal and vertical). Trial comes about demonstrate that for the situation that inserting strategy were known, the proposed technique can accomplish similarly great outcomes with the technique [23]. For the instance of reference framework recorded in the final section in each table, it is watched that there will even now be extraordinary opportunity to get better in all cases, which implies that assessing the modifications was the most vital

issue in the proposed versatile steganalysis and that it significantly influences the effectiveness of the proposed procedure.

Embedding Rate	**SRM required/ effectiveness (in %)**	**Effective Pixel accounted with embedding (in %)**				**Detection Resistance (in %)**
		10	**20**	**35**	**50**	
0.05 bpp	30.98	20.81	20.70	20.40	20.30	12.0
0.10 bpp	23.21	16.76	16.22	16.07	15.87	9.30
0.20 bpp	14.37	11.13	11.09	11.07	10.96	6.76
0.30 bpp	9.67	8.85	8.56	8.50	8.45	5.20
0.40 bpp	6.61	6.40	6.39	6.27	6.26	3.82
0.50 bpp	4.95	4.77	4.74	4.72	4.70	2.82

Table 5.4 Detection errors for EA Steganography based on re-embedding random experiments

Embedding Rate	**SRM required/ effectiveness (in %)**	**Effective Pixel accounted with embedding (in %)**				**Detection Resistance (in %)**
		10	**20**	**35**	**50**	
0.05 bpp	25.69	23.87	23.67	22.75	22.53	20.10
0.10 bpp	20.79	18.98	18.75	18.45	17.82	16.54
0.20 bpp	13.56	12.54	11.45	11.34	11.12	10.32
0.30 bpp	9.67	9.54	8.89	8.56	8.34	7.29
0.40 bpp	6.45	6.34	6.29	6.21	5.79	4.12
0.50 bpp	4.73	4.65	4.45	4.32	4.24	2.89

Table 5.5 Detection errors for WOW Steganography based on re-embedding random experiments

Embedding Rate	SRM required/ effectiveness (in %)	Effective Pixel accounted with embedding (in %)				Detection Resistance (in %)
		10	20	35	50	
0.05 bpp	22.39	20.89	20.67	19.79	19.54	19.82
0.10 bpp	19.76	18.98	18.77	17.86	17.34	16.65
0.20 bpp	15.54	13.49	13.34	12.84	12.55	11.43
0.30 bpp	9.45	8.69	7.56	7.34	7.21	6.78
0.40 bpp	6.66	6.56	6.43	6.23	6.07	5.31
0.50 bpp	4.34	4.29	4.23	4.17	4.12	2.67

Table 5.6 Detection errors for HUGO BD Steganography based on re-embedding random experiments

Embedding Rate	SRM required/ effectiveness (in %)	Effective Pixel accounted with embedding (in %)				Detection Resistance (in %)
		10	20	35	50	
0.05 bpp	25.68	22.78	21.88	21.75	21.45	24.50
0.10 bpp	21.34	19.97	18.84	18.75	18.69	17.75
0.20 bpp	18.45	17.97	17.83	16.67	16.34	15.57
0.30 bpp	13.32	11.57	11.34	10.78	10.45	8.93
0.40 bpp	7.23	6.98	6.75	6.53	6.34	4.45
0.50 bpp	4.94	4.78	4.65	4.53	4.42	2.43

Table 5.7 Detection errors for S-UNIWARD Steganography based on re-embedding random experiments

Embedding Rate	SRM required/effectiveness (in %)	Effective Pixel accounted with embedding (in %)				Detection Resistance (in %)
		10	20	35	50	
0.05 bpp	26.19	24.69	23.97	23.73	23.47	25.69
0.10 bpp	22.21	18.76	18.45	17.86	17.43	16.83
0.20 bpp	17.42	15.79	15.45	14.84	14.63	13.49
0.30 bpp	13.42	12.94	12.67	12.53	12.32	11.57
0.40 bpp	9.94	8.88	8.64	8.42	8.13	7.44
0.50 bpp	5.89	5.75	5.64	5.34	5.14	3.23

Table 5.8 Detection errors for LSB-MATCHING Steganography based on re-embedding random experiments

5.2.2 Acquiring Embedding Probabilities Based on Re-Embedding Random Experiments:

Take note of that the ideal test system may not work when the steganographic strategy isn't outlined under the structure of limiting the bending capacity, for example, EA steganography. All things considered, can evaluate likelihood maps in view of re-inserting arbitrary investigations as takes after. For a given picture, with the acquired right steganographic programming, implants an arbitrary message with a given inserting rate autonomously M times and afterward tally how often every pixel in the position (i, j) had been modified after the M times irregular analyses, meant as $(N_{i,j})$. At last the implanting likelihood of this pixel can be assessed by $(N_{i,j}/M)$. For this situation, the quantity of arbitrary examinations M was an essential parameter. In the investigations, parameter M going from 1 to 50 had been tried. Table 5.4 demonstrates the exploratory outcomes for the EA technique. From Table 5.4 it can be seen that the discovery blunders generally diminish as parameter M increments. In [7], the underscores that were in iterative steganalysis, were imperative to know the quantity of emphasess, i.e. M, which can be found by comprehensive hunt. Through comprehensive pursuit, found that when M was bigger than 7, the proposed strategy were beaten by the first SRM technique for all installing rates. The change was significant particularly when the implanting rate were low. Taking 0.05 bpp for instance, were accomplish as high as 10% change when parameter $M \geq 7$. Moreover, it can likewise be seen that the change winds up minor (the distinction is under 0.14%) when M was bigger than 40. In this way, it was suggested that parameter M ought not be under 40. Table 5.5, 5.6 ,5.7 and 5.8 demonstrates the trial comes about for WOW, HUGO BD, S-UNIWARD and LSB-matching assessed. Also, the location blunders diminish as parameter M increments. The proposed strategy outflanks the first SRM when $M \geq 10$. From Tables 5.5, 5.6 ,5.7 and 5.8 it can likewise be seen that the recognition blunders in light of re-implanting arbitrary investigations turn out to be fundamentally the same as (the distinction is under 0.29%) to the comparing comes about utilizing the ideal test system (see the final segment) when parameter $M \geq 40$.

5.2.3 Investigation of Mismatched Probabilities Conditions:

When the embedding algorithm was unknown, the method based on optimal simulator may encounter mismatched probabilities conditions since getting the weights with the optimal simulator was dependent on the steganographic algorithm (e.g., the embedding probabilities). When the mismatched embedding probabilities were used, the detection error will increase significantly. For example, if the embedding probabilities estimated with the HUGO BD steganographic method were used to set weights to detect the WOW stego images with SRM features, the corresponding detection errors would increase significantly from 20.10% (the matched case) to 24.84% (the mismatched case). However, if it can obtain the right steganographic software, the re-embedding method can still estimate the embedding probabilities accurately even though it did not know any details about the embedding algorithm. Actually, the mismatch probabilities can be regarded as a noisy version of the actual embedding probabilities.

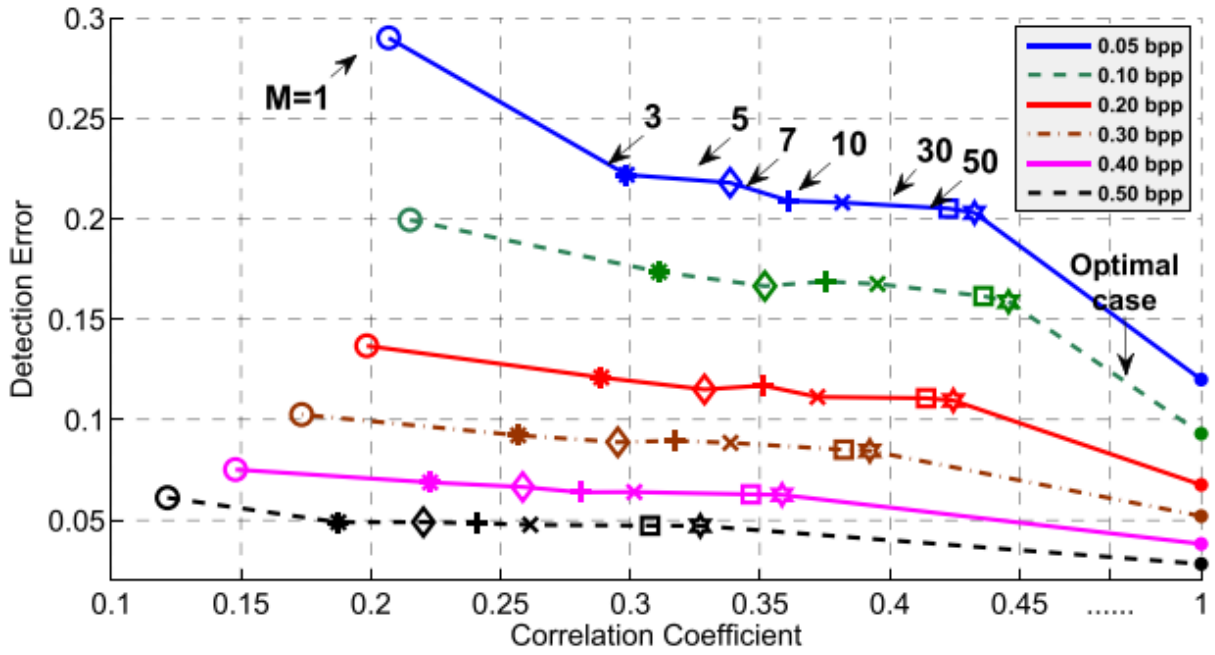


Figure 5.5 Behavior curve of LSB Steganography technique with respect to detection error versus correlation coefficient

5.3 Discussions:

This section contains, the analysis of a few factors that influence the discovery execution of the different versatile plan.

5.3.1 Execution Analysis with Correlation Test:

As depicted, it was conceivable to the areas of modified pixels with the assistance of installing probabilities. It was normal that the more exact areas were evaluated, the better the change were gotten, as the proposed versatile highlights could catch more supportive data about the modifications presented by information inserting. In this subsection, it was dissected that the adequacy of the versatile steganalysis depended on a connection test. In these analyses, it plainly demonstrated the connection between identification mistakes and relationship coefficients. The investigations was assessed in view of 10,000 pictures from BOSS base were appeared in Figure 5.5. For each point in Figure 5.5, the x-axis indicates the normal consequence of the connection coefficients between the weight vectors and the modification vectors for more than 10,000 pictures, and the y-axis means the normal location mistakes for more than 10,000 pictures. Three strategies including the past versatile strategy [28] and the reference framework were considered. The connection coefficient was a measure of the level of straight connection between the weights and the modifications after information covering up, and in this way a bigger relationship coefficient implies were assessed and the modified pixels were more precise, which truely shows the

accomplishment and greater change. The identification blunder achieves the base values if the connection coefficient achieves the greatest estimation of 1. The trial comes about appeared in Figure 5.5 coordinate the examined results exceptionally well. In view of the above examinations and investigations, it was noticed that how the areas of the modified pixels were evaluated, and assumed a vital part in the proposed versatile steganalysis. The modifications after versatile steganography were generally situated in the textural districts, with the goal that it is conceivable to gauge these modifications all the more precisely for steganalysis. That was the reason the proposed system enhances the recognition execution in versatile steganography. Taking note of that the proposed technique can't enhance the location execution for non-versatile steganographic strategies, as the inserting probabilities of all pixels were precisely the same for this situation, and the connection coefficients were generally near zero. It would be ideal if taken note of that like most current steganalytic strategies, for example, SRM [6] and LBP-based technique [29], that conspires does not consider CSM [12] issues, (for example, obscure steganography and additionally implanting rate, obscure picture sources).

5.3.2 Robustness Analysis Against Noise Contamination:

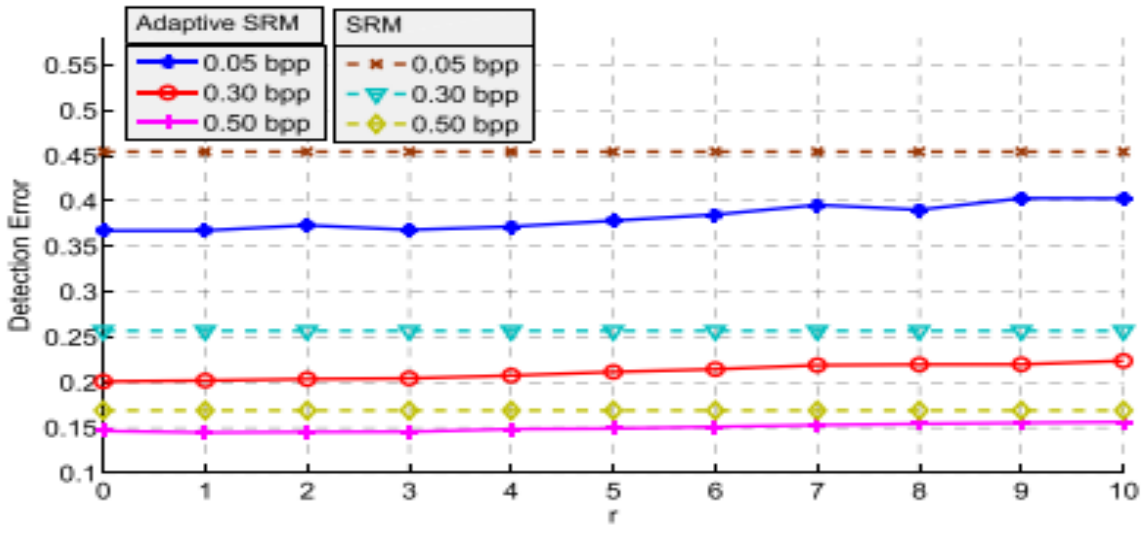
In view of trials, it was realized that the identification execution of the proposed plot was subject to the assessed installing probabilities. In this subsection, it will be demonstrated how does the location execution change when the implanting probabilities were sullied by commotion. Three reenactment investigations of two various types of clamor, i.e., spatial jitter and value metric commotion (counting multiplicative and added substance cases) have been led. The utilization the images P and $(P_{i,j})$ to mean the likelihood delineate by the ideal test system and the likelihood esteem situated at the position (i, j) in the guide; and utilize P and $P_{i,j}$ to indicate the comparing guide and incentive after clamor pollution.

1) Spatial Jitter: For the situation of spatial jitter, the first likelihood $P_{i,j}$ is arbitrarily supplanted by its neighboring component $P_{i+ni,j+nj}$ to get the loud likelihood $P_{i,j}$. In the investigations, clamor bending was acquired, the uproarious likelihood were as per the following:

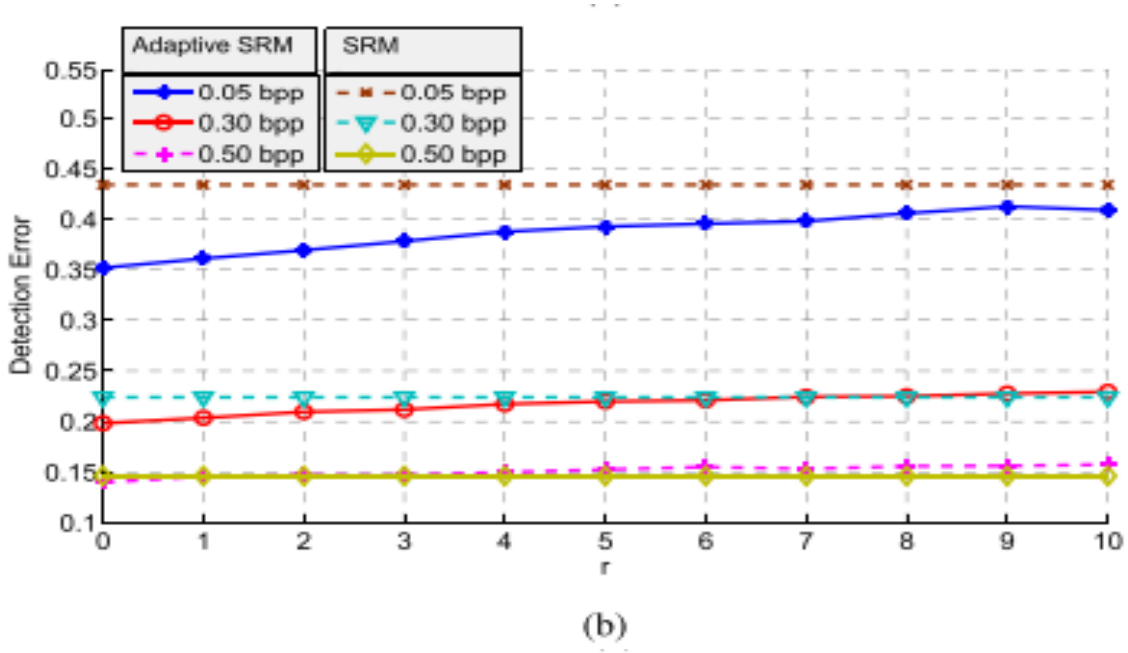
$$P_{i,j} = P_{i+ni\,,j+nj}$$

where the binary conveyance of (n_i, n_j) was a uniform circulation around with the span r and the middle (0, 0). Here, the parameter r is utilized to control the quality of the spatial jitter, and set r running from 0 to 10 with a stage 1 in the tests. From figure 5.7, it was watched that the recognition mistakes for the three steganography will increment with expanding the parameter r, particularly when the inserting rate is low. For example, when the inserting rate is 0.05 bpp, the expansion of discovery mistakes for WOW, HUGO BD and S-UNIWARD are 3.52%, 4.80%, and 1.40% with r expanding from 0 to 10, showing that the more quality of spatial jitter, the poorer identification execution were acquired. For similar investigations, likewise demonstrated the execution of the first non-versatile SRM. It can be seen that as a rule, the

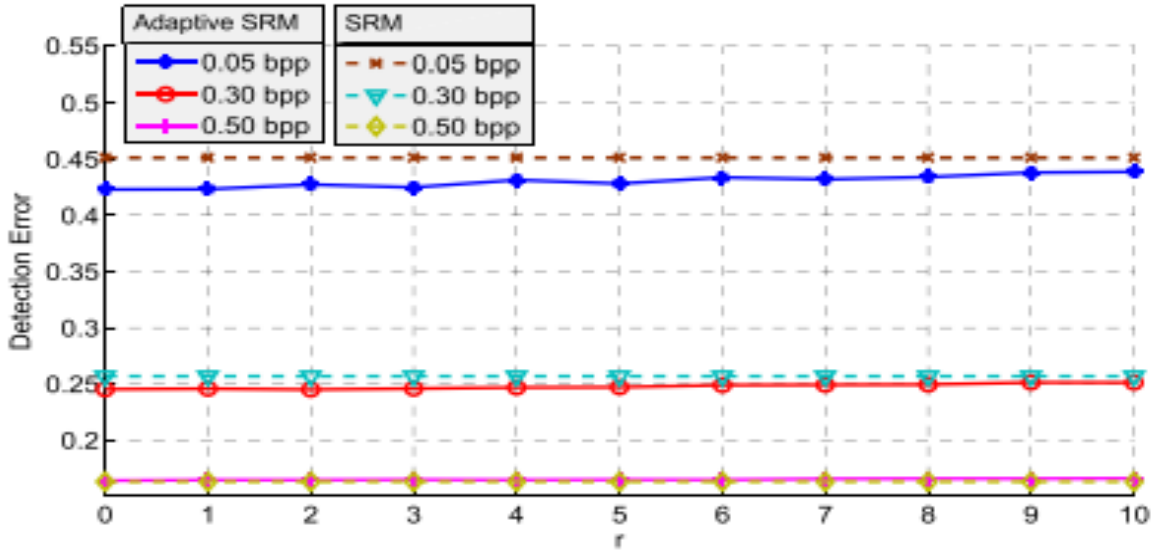
versatile SRM tainted by spatial jitter still would do well to execution than the first non-versatile SRM. Be that as it may, now and again, for example, HUGO BD on 0.50 bpp, the location mistake of the versatile SRM undermined by spatial jitter with commotion quality 10 is higher than the first non-versatile SRM by 1.1%. It is likewise watched that contrasted with WOW and HUGO BD, S-UNIWARD appears to be more hearty against the spatial jitter. To clarify such a perception, the accompanying investigation was directed. For a given picture, the firstly the likelihood outline was partitioned into 10 × 10 covering squares, and afterward computed the difference for the probabilities in each square. At least, the mean estimation of the fluctuation of all squares in the picture were gotten. It was normal that for those versatile steganography whose likelihood outline littler mean estimation of neighborhood difference, their nearby probabilities were more comparable, and along these lines they were more vigorous against the spatial jitter. As demonstrated the normal of the mean estimations of nearby change of the probabilities from 10×10 squares more than 10,000 pictures from BOSS base and the comparing increment of location mistakes for three diverse steganographic techniques while expanding r from 0 to 10. The trial outcomes fit the examination extremely well.



(a)



(b)



(c)

Figure 5.6 Detection error versus spatial jitter (a) WOW, (b) HUGO BD (c) S-UNIWARD respectively.

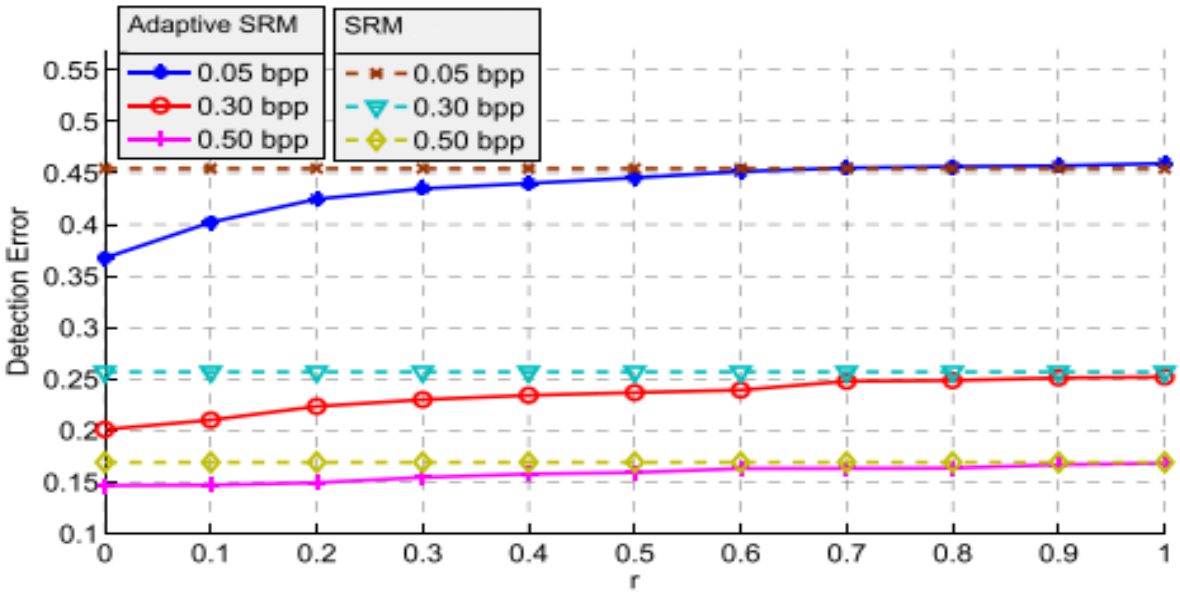
2) Multiplicative Noise: For the situation of multiplicative clamor, each unique likelihood ($P_{i,j}$) was duplicated by an irregular variable autonomously. In these trials, the uproarious likelihood was acquired as takes after:

$$P'_{i,j} = (P_{i,j})(n_{i,j})$$

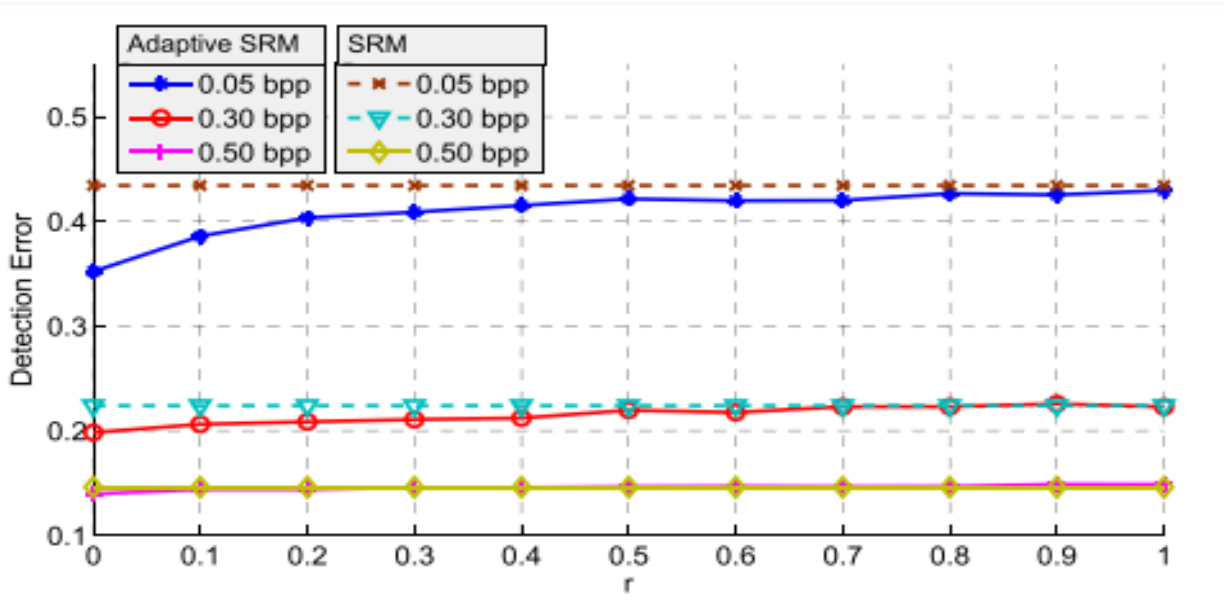
where $(n_{i,j})$ was a free and indistinguishable dispersed irregular variable from a uniform conveyance in the scope of $[0, r]$. The parameter r indicates the quality of the multiplicative commotion. It should be noted that because of the standardization task in SRM [6], it was anything but difficult to demonstrate that distinctive estimations of multiplicative commotion qualities i.e., diverse a, makes no distinctions to the

versatile SRM highlights, if overlooking the adjusting blunder in computation. In view of the broad analyses, it was likewise discovered that the identification execution for various r going from 0.1 to 1,000 is very comparable (under 0.3% in light of our investigations). In this manner, by setting r as 1 and demonstrate the normal location comes about more than 10 arbitrary analyses. It was watched that the multiplicative clamor had little impact on the recognition execution (under 0.54% in all cases). The conceivable reason was that the weight was gotten as the mean estimation of four nearby pixels probabilities in the technique, which would smoother the multiplicative commotion successfully. In this way, that likelihood delineate increased by arbitrary commotion consistently dispersed between $[0, r]$ does not break the versatile steganalysis framework

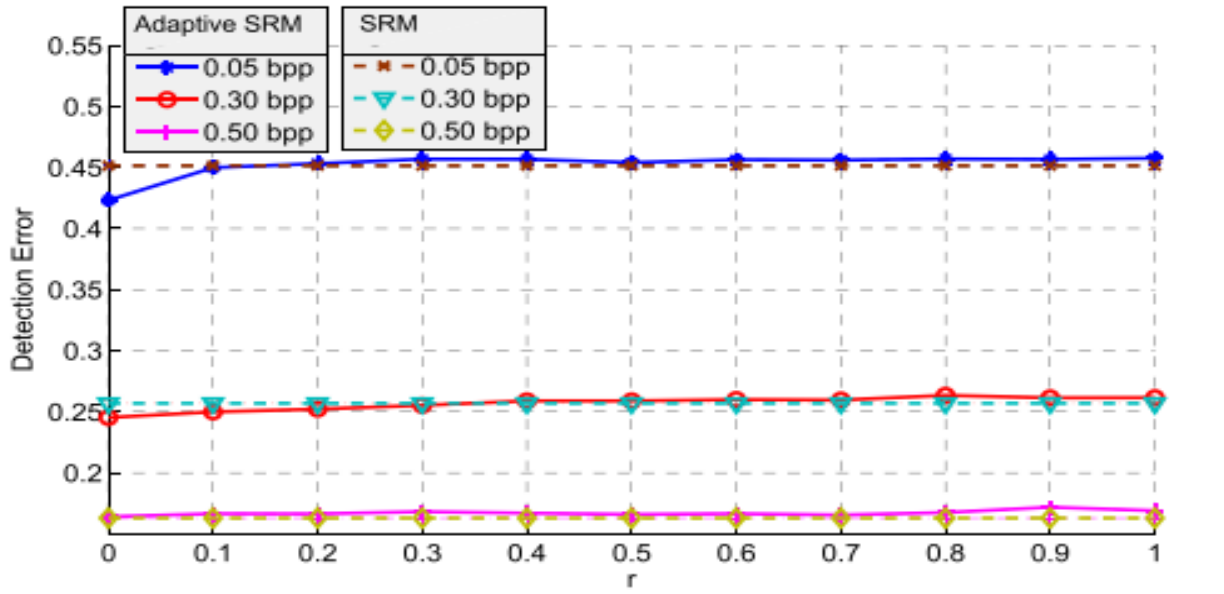
.



(a)



(b)



(c)

Figure 5.7 Detection error versus gradual increment in additive noise (a) WOW (b) HUGO BD (c) S-UNIWARD respectively.

3) Additive Noise: For the situation of added substance commotion, each unique likelihood pi,j was included by an arbitrary variable freely. In the analyses, it acquired the noisy likelihood as taken after: where $(n_{i,j})$ is a free and indistinguishable appropriated irregular variable from a uniform dispersion in the scope of $[-r, r]$, the truncation activity truncates the subsequent qualities into [0,1] keeping in mind

the end goal to coordinate the physical significant of likelihood. Here, the parameter r were utilized to control the quality of the added substance clamor, and set r extending from 0 to 1 with a stage 0.1 in the trials. The normal identification comes about more than 5 arbitrary analyses were appeared in Figure 5.8. From Fig 5.8, it was watched that the location mistakes tended to increment with expanding the parameter r for all bends and step by step way to deal with the identification blunders of non-versatile SRM and might be considerably higher at times, for example, identifying S-UNIWARD when the clamor quality was high. The expansion of recognition blunders would end up littler when the payloads are higher, for example, 0.3 bpp and 0.5 bpp. For instance, as appeared, with expanding r from 0 to 1, the expansion of location mistakes for WOW are 8.72%, 4.18%, and 2.13% on 0.05 bpp, 0.30 bpp, and 0.50 bpp. The reason might be that in the ideal test system, the higher payload for the most part prompts bigger implanting likelihood. While including a similar quality of added substance commotion ni,j into pi,j with various payloads, the extent amongst clamor and likelihood (i.e., $n_{i,j}/P_{i,j}$) was littler when the payload was higher, and accordingly the expansion of recognition mistakes was littler for this situation. In view of the above reenactment tries, the three after perceptions were made:

i) The multiplicative commotion scarcely influences the location execution of the proposed versatile steganalysis against the three steganographic techniques.
ii) For the spatial jitter and the added substance commotion, the location mistakes would increment with expanding the quality of clamor, particularly when the implanting rate is low, e.g., 0.05 bpp. Be that as it may, for high implanting rates, for example, 0.3 bpp and 0.5 bpp, the increments of recognition mistakes were generally littler contrasted with the relating instance of 0.05 bpp.
iii) The expansion of discovery blunders for S-UNIWARD were moderately littler contrasted with the outcomes for WOW and HUGO BD under the same implanting rate, a similar kind of commotion and a similar clamor quality.
iv) The execution of the adapitve steganalysis might be poorer than non-versatile steganalysis when the probabilities were debased by spatial jitter or added substance clamor with high commotion quality.

5.4 Further comparison between Initial and Innovated LSB based steganographic approach:

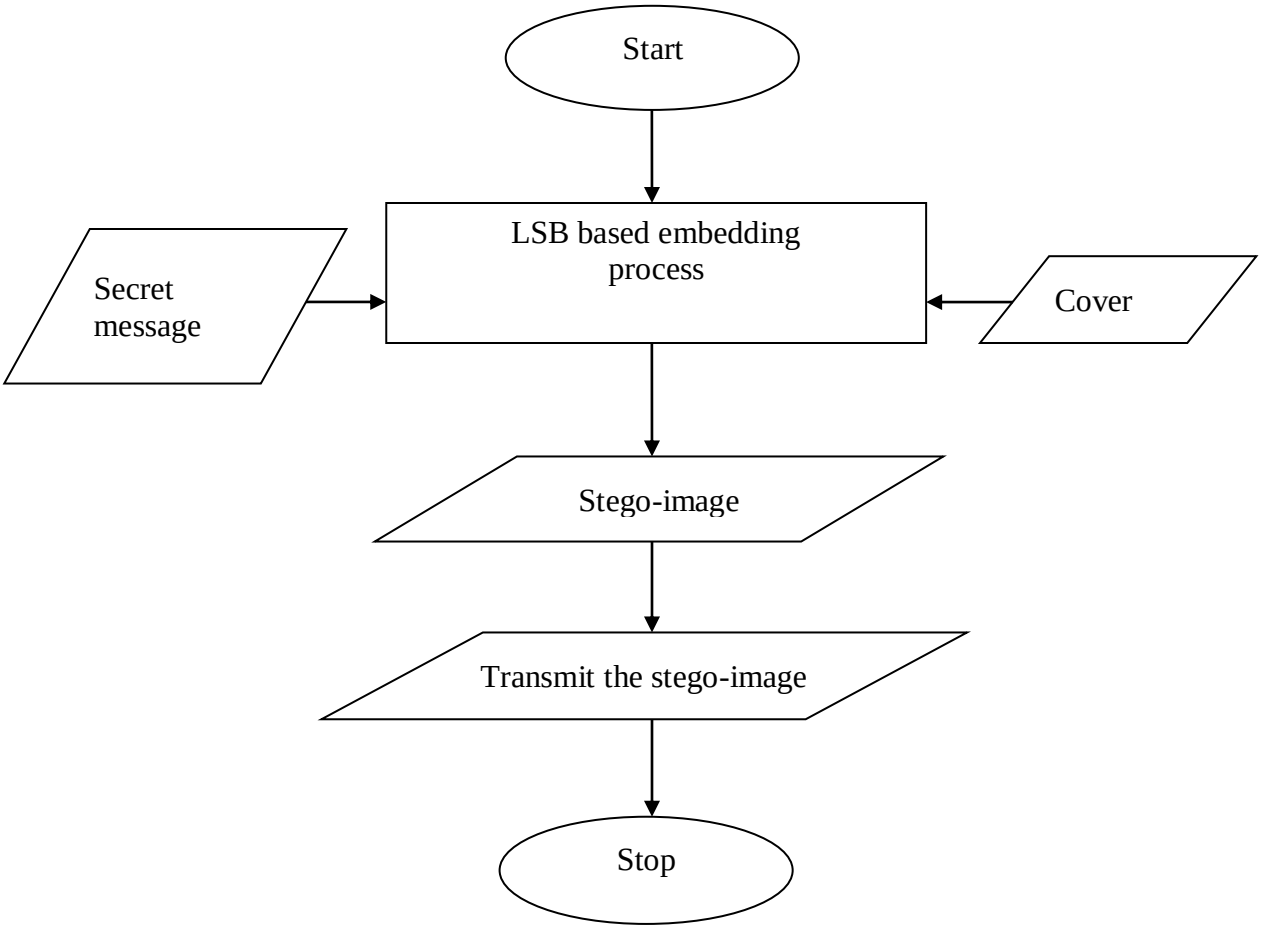


Fig 5.8 Initial approach

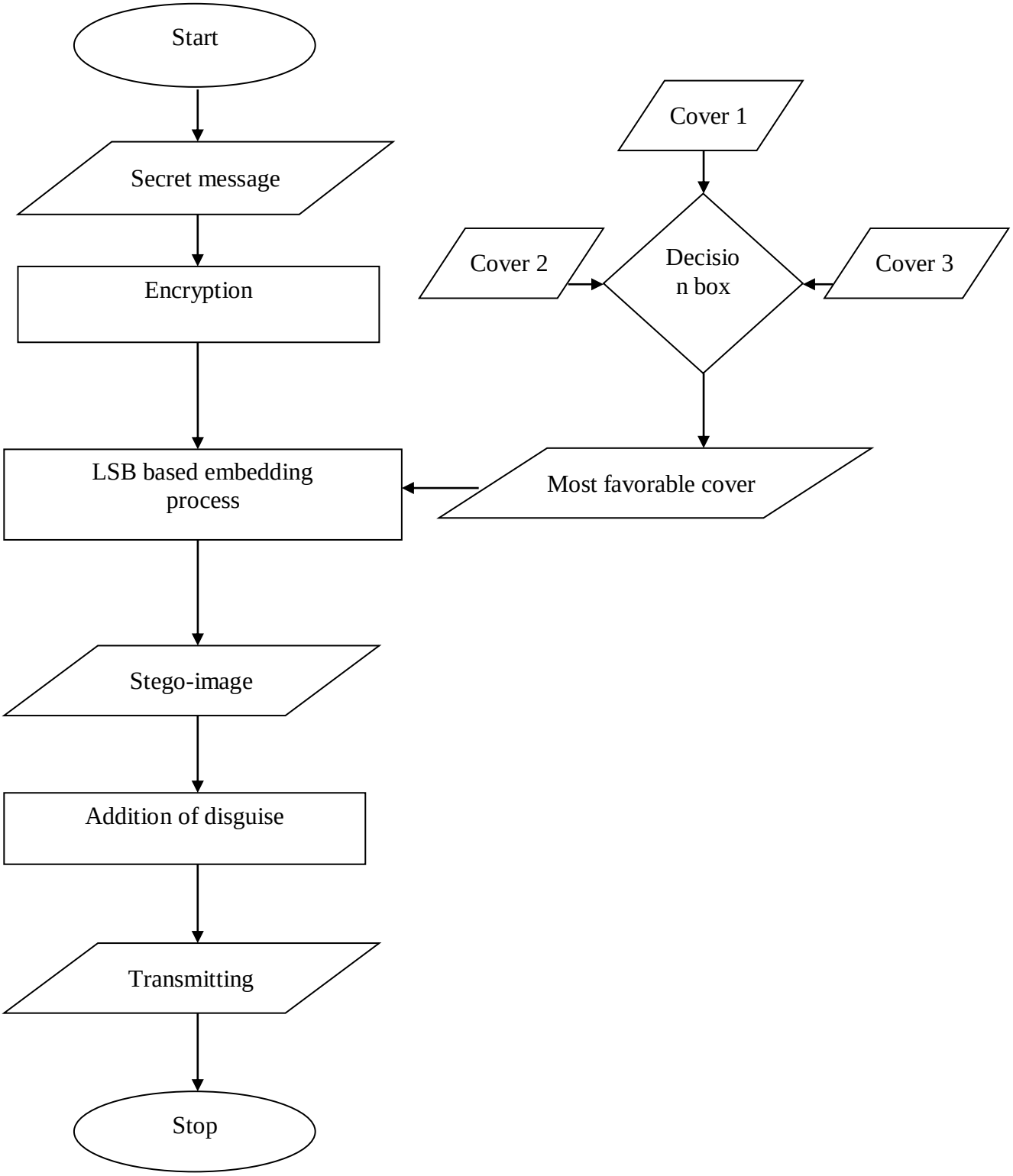


Figure 5.9 : Developed approach

Sr .No	Initial approach (figure 5.1)	Developed approach (figure 5.2)
1	The approach is simpler in structure and involve less steps.	The approach is relatively complex and involve number of steps.
2	No pre-encryption present.	Pre-encryption is present.
3	The approach do not have a suitable cover selection process.	The approach involves suitable cover selection process.
4	No disguise is added before transmission.	Suitable disguise is added before transmission.
5	Time taken by the approach is comparatively less.	Time taken by the approach is comparatively more.
6	Security level of approach is low.	Security level of approach is comparatively higher.
7	Once the image gets detected the entire approach fails.	The approach doesn't fails entirely after image detection.
8	The approach is comparatively less efficient.	The approach is comparatively more effecient.
9	Due to lack in security the approach requires a separate or highly secured channel for transmission.	This approach doesn't need any separate or highly secured channel for transmission.
10	Overall the cost of this approach is less due to involvement of less infrastructure.	Overall the cost of this approach is high due to involvement of more infrastructure.

Table 5.9: Comparison between initial and developed approach

5.5 Concluding remarks:

Based on the information and results from simulation result from section 5.1, it can be concluded that LSB based steganography technique is one of the most simple and economic technique as compare to others and it is far more suitable for communicating in commercial targets with not so high priority. In case of high value target achievement it is needed to make so remarks to improve its performance and scale of security. The following are some remarks which can be added:

- Encrypting of message pre from coding and transmitting so that anyone who decodes it must also decrypt it before it makes any sense.
- Pseudo random noise is also be added to it which makes it impossible to decrypt without have the type of pseudo random noise generator and it corresponding peers and algorithm.
- File size is to be kept a minimal magnitude, so as the embedding could be swift, effective and undetectable for general purposes 8bit image should be employed rather than large magnitude media as it would cause suspicion.
- The disadvantage in employing a high defined (HD) media is its excellent definition for the concept of steganography. To work properly/effectively the image definition should not be very high so as the secret embedded message could be disguised efficiently and undetectable within the media and should be detectable by human senses (eyes/ears). Therefore media or image higher definition say (256) or higher should not be embedded or be used for any steganographic purpose.

5.6 Future scope:

Steganographic techniques can be and are used in many fields now a days. Say be it :

- In marketing in coupons and cards with various gifts and offers.
- In medical science to keep the confidentiality of the report between doctor and patient.
- In research field to keep the ideas and research delivered to the desired person only.
- In organizations and multi-national corporations to keep the details to business confidential.
- In military to share the secrets of defense and arms and national security.

References

[1] M. Boroumand and J. Fridrich, (2018) "Applications of Explicit Non-Linear Feature Maps in Steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 823-833.

[2] B. Li, Z. Li, S. Zhou, S. Tan and X. Zhang, (2018) "New Steganalytic Features for Spatial Image Steganography Based on Derivative Filters and Threshold LBP Operator," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1242-1257.

[3] Y. T. Lin, C. M. Wang, W. S. Chen, F. P. Lin and W. Lin, (2018)"A Novel Data Hiding Algorithm for High Dynamic Range Images," *IEEE Transactions on Multimedia*, vol. 19, no. 1, pp. 196-211.

[4] J. Zeng, S. Tan, B. Li and J. Huang, (2018)"Large-Scale JPEG Image Steganalysis Using Hybrid Deep-Learning Framework," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1200-1214.

[5] A. Abuadbba and I. Khalil, (2017) "Walsh–Hadamard-Based 3-D Steganography for Protecting Sensitive Information in Point-of-Care," *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 9, pp. 2186-2195.

[6] J. Camenisch, A. Lehmann, G. Neven and K. Samelin, (2017) "UC-Secure Non-interactive Public-Key Encryption," *IEEE 30th Computer Security Foundations Symposium (CSF)*, Santa Barbara, CA, pp. 217-233.

[7] T. Denemark and J. Fridrich, (2017) "Steganography With Multiple JPEG Images of the Same Scene," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2308-2319.

[8] K. Huang and R. Tso, (2017) "Provable secure dual-server public key encryption with keyword search,"*IEEE 2nd International Verification and Security Workshop (IVSW)*, Thessaloniki, pp. 39-44.

[9] Q. Kong, R. Lu, S. Chen and H. Zhu, (2017) "Achieve Secure Handover Session Key Management via Mobile Relay in LTE-Advanced Networks," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 29-39.

[10] M. Ma, D. He, N. Kumar, K. K. R. Choo and J. Chen, (2017) "Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. no. 99, pp. 1-1.

[11] F. Pelcastre Jimenez, *et.al.* (2017) "An Inverse Halftoning Algorithms Based on Neural Networks and Atomic Functions," *IEEE Latin America Transactions*, vol. 15, no. 3, pp. 488-495.

[12] Z. Peng and S. Tang, (2017) "Circulant Rainbow: A New Rainbow Variant With Shorter Private Key and Faster Signature Generation," *IEEE,* vol. 5, pp. 11877-11886, 2017.

[13] I. G. Ray and M. Rajarajan, (2017) "A Public Key Encryption Scheme for String Identification," *IEEE Trust com /Big Data SE/ICESS*, Sydney, NSW, pp. 104-111.

[14] S. Tan, H. Zhang, B. Li and J. Huang, (2017) "Pixel-Decimation-Assisted Steganalysis of Synchronize-Embedding-Changes Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1658-1670.

[15] W. Tang, S. Tan, B. Li and J. Huang, (2017) "Automatic Steganographic Distortion Learning Using a Generative Adversarial Network," *IEEE Signal Processing Letters*, vol. 24, no. 10, pp. 1547-1551.

[16] Y. Wang and K. She, (2017)"A practical quantum public-key encryption model," *3rd International Conference on Information Management (ICIM)*, Chengdu, 2017, pp. 367-372.

[17] X. Wang, G. Zhou, C. Dai and J. Chen, (2017) "Optical Image Encryption With Divergent Illumination and Asymmetric Keys," *IEEE Photonics Journal*, vol. 9, no. 2, pp. 1-8.

[18] J. Wang, J. Ni, X. Zhang and Y. Q. Shi, (2017) "Rate and Distortion Optimization for Reversible Data Hiding Using Multiple Histogram Shifting," *IEEE Transactions on Cybernetics*, vol. 47, no. 2, pp. 315-326.

[19] Z. Wang, (2017) "An Identity-Based Data Aggregation Protocol for the Smart Grid," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2428-2435.

[20] Z. Wei, *et.al.* (2017) "HIBS-KSharing: Hierarchical Identity-Based Signature Key Sharing for Automotive," *IEEE*, vol. 5, pp. 16314-16323.

[21] Y. Xu, *et.al.* (2017) "Verifiable Public Key Encryption Scheme With Equality Test in 5G Networks," *IEEE*, vol. 5, pp. 12702-12713.

[22] J. Ye, J. Ni and Y. Yi, (2017) "Deep Learning Hierarchical Representations for Image Steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545-2557, 2017

[23] W. Zhang, *et.al.* (2017) "Decomposing Joint Distortion for Adaptive Steganography, " *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 27, no. 10, pp. 2274-2280.

[24] H. Zhang, *et.al.* (2017) "Multi-Key Generation Over a Cellular Model With a Helper, " *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 3804-3822.

[25] H. Zhou, (2017) “Steganography Using Reversible Texture Synthesis”, " *IEEE Transactions on Image Processing*, vol. 26, no. 4, pp. 1623-1625.

[26] W. Zhou, W. Zhang and N. Yu, (2017) "A New Rule for Cost Reassignment in Adaptive Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2654-2667.

[27] C. Zuo, et.al. (2017) "Hidden-Token Searchable Public-Key Encryption, " *IEEE Trust com/ Big Data SE/ ICESS*, Sydney, NSW, 2017, pp. 248-254.

[28] A. Santos Brandao and D. Calhau Jorge, (2017) "Artificial Neural Networks Applied to Image Steganography," *IEEE Latin America Transactions*, vol. 14, no. 3, pp. 1361-1366.

[29] R. Chen, *et.al.* (2016) "Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 789-798.

[30] R. Chen, *et al*. (2016) "Server-Aided Public Key Encryption With Keyword Search, " *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2833-2842, 2016.

[31] S. Chen, *et.al*. (2016) "Automatic Detection of Object-Based Forgery in Advanced Video, " *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 26, no. 11, pp. 2138-2151.

[32] T. D. Denemark, M. Boroumand and J. Fridrich, (2016) "Steganalysis Features for Content-Adaptive JPEG Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1736-1746.

[33] J. Duda, *et.al.* (2016) "Image-Like 2D Barcodes Using Generalizations of the Kuznetsov–Tsybakov Problem," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 691-703.

[34] D. He, *et.al.* (2016) "Efficient and Anonymous Mobile User Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server Architectures," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2052-2064, 2016.

[35] F. Huang, J. Huang and Y. Q. Shi, (2016) "New Framework for Reversible Data Hiding in Encrypted Domain," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2777-2789.

[36] F. Li, *et.al.* (2016) "Steganalysis Over Large-Scale Social Networks With High-Order Joint Features and Clustering Ensembles," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 344-357, 2016.

[37] K. Ntalianis and N. Tsapatsoulis, (2016) "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 156-174, 2016.

[38] J. R. Carneiro Tavares and F. Madeiro Bernardino Junior, (2016) "Word-Hunt: A LSB Steganography Method with Low Expected Number of Modifications per Pixel," *IEEE Latin America Transactions*, vol. 14, no. 2, pp. 1058-1064.

[39] V. Sedighi, R. Cogranne and J. Fridrich, (2016) "Content-Adaptive Steganography by Minimizing Statistical Detectability," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 221-234.

[40] H. Tan, *et.al.* (2016) "A Secure and Authenticated Key Management Protocol (SA-KMP) for Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9570-9584.

[41] W. Tang, *et.al.* (2016) "Clustering Steganographic Modification Directions for Color Components," *IEEE Signal Processing Letters*, vol. 23, no. 2, pp. 197-201.

[42] W. Tang, *et.al.* (2016) "Adaptive Steganalysis Based on Embedding Probabilities of Pixels," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 734-745.

[43] Xianyi Chen, *et.al.* (2016) "Steganalysis of LSB matching using characteristic function moment of pixel differences," in *China Communications*, vol. 13, no. 7, pp. 66-73.

[44] G. Xu, H. Z. Wu and Y. Q. Shi, (2016) "Structural Design of Convolutional Neural Networks for Steganalysis, " *IEEE Signal Processing Letters*, vol. 23, no. 5, pp. 708-712.

[45] J. Yu, *et.al.* (2016) "Spatial Steganalysis Using Contrast of Residuals," *IEEE Signal Processing Letters*, vol. 23, no. 7, pp. 989-992.

[46] W. Zhang, *et.al.* (2016) "Reversible Data Hiding in Encrypted Images by Reversible Image Transformation," *IEEE Transactions on Multimedia*, vol. 18, no. 8, pp. 1469-1479.

[47] J. H. Cheon and J. Kim, (2015) "A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1052-1063.

[48] R. Cogranne and J. Fridrich, (2015) "Modeling and Extending the Ensemble Classifier for Steganalysis of Digital Images Using Hypothesis Testing Theory," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2627-2642.

[49] B. Feng, W. Lu and W. Sun, *et.al.* (2015) "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 243-255.

[50] L. Guo, *et.al.* (2015)"Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2669-2680.

[51] V. Holub and J. Fridrich, (2015) "Low-Complexity Features for JPEG Steganalysis Using Undecimated DCT," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 219-228.

[52] B. Li, *et.al.* (2015) "A Strategy of Clustering Modification Directions in Spatial Image Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1905-1917.

[53] S. Ma, *et.al.* (2015) "Efficient Public Key Encryption With Equality Test Supporting Flexible Authorization," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 458-470.

[54] M. M. E. A. Mahmoud, et.al. (2015) "Investigating Public-Key Certificate Revocation in Smart Grid," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 490-503.

[55] Y. M. Tseng and T. T. Tsai, (2015) "Efficient Revocable ID-Based Encryption with a Public Channel," *The Computer Journal*, vol. 55, no. 4, pp. 475-486.

[56] K. C. Wu and C. M. Wang, (2015) "Steganography Using Reversible Texture Synthesis," *IEEE Transactions on Image Processing*, vol. 24, no. 1, pp. 130-139.

[57] L. Guo, J. Ni and Y. Q. Shi, (2015) "Uniform Embedding for Efficient JPEG Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 814-825.

[58] J. Kodovsky and J. Fridrich, (2014) "Effect of Image Downsampling on Steganographic Security," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 752-762.

[59] B. Li, et.al. (2014) "Investigation on Cost Assignment in Spatial Image Steganography, " *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, pp. 1264-1277.

[60] X. Ma, *et.al.* (2014) "JPEG-compatibility steganalysis that distinguishes embedding changes from recompression artifacts," *China Communications*, vol. 11, no. 9, pp. 173-182.

[61] H. Nicanfar, et.al. (2014) "Efficient Authentication and Key Management Mechanisms for Smart Grid Communications," *IEEE Systems Journal*, vol. 8, no. 2, pp. 629-640.

[62] T. H. Thai, R. Cogranne and F. Retraint, (2014) "Statistical Model of Quantized DCT Coefficients: Application in the Steganalysis of Jsteg Algorithm," *IEEE Transactions on Image Processing*, vol. 23, no. 5, pp. 1980-1993.

[63] K. Wang, H. Zhao and H. Wang, (2014) "Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 741-751.

[64] B. Dai, *et.al.* (2013) "Orthogonal DPSK/CSK Modulation and Public-Key Cryptography-Based Secure Optical Communication," *IEEE Photonics Technology Letters*, vol. 25, no. 19, pp. 1897-1900.

[65] G. Gul and F. Kurugollu, (2013) "JPEG Image Steganalysis Using Multivariate PDF Estimates With MRF Cliques," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 578-587.

[66] V. Holub and J. Fridrich, (2013) "Random Projections of Residuals for Digital Image Steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1996-2006.

[67] A.Ibaida and I. Khalil, (2013) "Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems," *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 12, pp. 3322-3330.

[68] F. Li, *et.al.* (2013) "JPEG Steganalysis With High-Dimensional Features and Bayesian Ensemble Classifier," *IEEE Signal Processing Letters*, vol. 20, no. 3, pp. 233-236.

[69] C. Qin, *et.al.* (2013) "An Inpainting-Assisted Reversible Steganographic Scheme Using a Histogram Shifting Mechanism," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 7, pp. 1109-1118.

[70] J. R. Shih, *et al*. (2013) "Securing M2M With Post-Quantum Public-Key Cryptography, " *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 106-116.

[71] L. Uhsadel, *et.al*. (2013) "Teaching HW/SW Co-Design With a Public Key Cryptography Application," *IEEE Transactions on Education*, vol. 56, no. 4, pp. 478-483, 2013.

[72] Y. Cao, X. Zhao and D. Feng, *et.al.* (2012) "Video Steganalysis Exploiting Motion Vector Reversion-Based Features," *IEEE Signal Processing Letters*, vol. 19, no. 1, pp. 35-38.

[73] Y. C. Chen, G. Horng and D. S. Tsai, *et.al.* (2012) "Comment on “Cheating Prevention in Visual Cryptography”," *IEEE Transactions on Image Processing*, vol. 21, no. 7, pp. 3319-3323.

[74] L. Fillatre, (2012) "Adaptive Steganalysis of Least Significant Bit Replacement in Grayscale Natural Images," *IEEE Transactions on Signal Processing*, vol. 60, no. 2, pp. 556-569.

[75] J. Fridrich and J. Kodovsky, (2012) "Rich Models for Steganalysis of Digital Images, " *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868-882.

[76] W. Hong and T. S. Chen, (2012) "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 176-184.

[77] F. Huang, J. Huang and Y. Q. Shi, (2012) "New Channel Selection Rule for JPEG Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1181-1191.

[78] J. Kodovsky, J. Fridrich and V. Holub, (2012) "Ensemble Classifiers for Steganalysis of Digital Media," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432-444.

[79] C. W. Lee and W. H. Tsai, (2012) "A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability," *IEEE Transactions on Image Processing*, vol. 21, no. 1, pp. 207-218.

[80] H. Malik, K. P. Subbalakshmi and R. Chandramouli, (2012) "Nonparametric Steganalysis of QIM Steganography Using Approximate Entropy," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 418-431.

[81] S. Tan and B. Li, (2012) "Targeted Steganalysis of Edge Adaptive Image Steganography Based on LSB Matching Revisited Using B-Spline Fitting," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 336-339.

[82] C. N. Yang, *et.al.* (2012) "Enhanced Matrix-Based Secret Image Sharing Scheme," *IEEE Signal Processing Letters*, vol. 19, no. 12, pp. 789-792.

[83] T. Filler, J. Judas and J. Fridrich, *et.al.* (2011) "Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 920-935.

[84] C. L. Hou, *et.al.* (2011)"An Optimal Data Hiding Scheme With Tree-Based Parity Check, " *IEEE Transactions on Image Processing*, vol. 20, no. 3, pp. 880-886.

[85] X. Luo, (2011) "On the Typical Statistic Features for Image Blind Steganalysis," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 7, pp. 1404-1422.

[86] W. Luo, Y. Wang and J. Huang, (2011) "Security Analysis on Spatial Steganography for JPEG Decompressed Images," *IEEE Signal Processing Letters*, vol. 18, no. 1, pp. 39-42.

[87] H. M. Sun, et.al. (2011) "Anti-Forensics with Steganographic Data Embedding in Digital Images," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 7, pp. 1392-1403.

[88] W. J. Wang, C. T. Huang and S. J. Wang, (2011) "VQ Applications in Steganographic Data Hiding Upon Multimedia Images," *IEEE Systems Journal*, vol. 5, no. 4, pp. 528-537.

[89] G. Gul and F. Kurugollu, (2010) "SVD-Based Universal Spatial Domain Image Steganalysis, " *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 349-353.

[90] J. M. Guo and T. N. Le, (2010) "Secret Communication Using JPEG Double Compression," *IEEE Signal Processing Letters*, vol. 17, no. 10, pp. 879-882.

[91] G. S. Lin, Y. T. Chang and W. N. Lie, (2010) "A Framework of Enhancing Image Steganography With Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm," *IEEE Transactions on Multimedia*, vol. 12, no. 5, pp. 345-357.

[92] W. Luo, F. Huang and J. Huang, (2010) "Edge Adaptive Image Steganography Based on LSB Matching Revisited," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 201-214.

[93] T. Pevny, P. Bas and J. Fridrich, (2010) "Steganalysis by Subtractive Pixel Adjacency Matrix," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 215-224.

[94] A.Sarkar, U. Madhow and B. S. Manjunath, (2010) "Matrix Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 225-239.

[95] J. Zhang and D. Zhang, (2010) "Detection of LSB Matching Steganography in Decompressed Images," *IEEE Signal Processing Letters*, vol. 17, no. 2, pp. 141-144.

[96] A. Kakkar, M. L. Singh, P. K. Bansal, (2012) "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network," *International Journal of Engineering and Technology*, vol. 2, no. 1, pp. 87-92.

[97] A. Kakkar, M. L. Singh, P. K. Bansal, (2010) "Efficient key mechanism in Multi-Node Network for Secured Data Transmission," *International Journal of Engineering Science and Technology*, vol. 2, pp. 787-795.

[98] A. Kakkar, M. L. Singh, P. K. Bansal, (2012) "Mathematical analysis and simulation of multiple keys and S-Boxes in a multinode network for secure transmission," *International Journal of Computer Mathematics*, vol. 89, pp. 2123-2142

[99] A. Kakkar, Manpreet Singh, Harpreet Kaur, (2015) "Digital Signature Verification Scheme for Image Authentication," *International Conference on Recent Advances in Engineering & Computational Sciences (RAECS),"* Punjab University, Punjab, India, pp.1-5.

[100] A. Kakkar, Tejbir kaur, (2017) "Sharing of Digital Secret Image by Diverse Media for more Security," M.E. Thesis, Thapar University, Patiala.

List of Publications

- S. Kaushal and A. Kakkar, (2018) "LSB based Steganography Techniques for Secured Communication," *Internatinal Journal of Computer Applications,* vol. 181, no. 10, pp. 28-31.

LSB based Steganography Techniques for Data Transmission Security

ORIGINALITY REPORT

9%	3%	8%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Harrisburg University of Science and Technology Student Paper	1%
2	Xia, Zhihua, Xinhui Wang, Xingming Sun, Quansheng Liu, and Naixue Xiong. "Steganalysis of LSB matching using differences between nonadjacent pixels", Multimedia Tools and Applications, 2014. Publication	1%
3	Kaibin Huang, Raylin Tso. "Provable secure dual-server public key encryption with keyword search", 2017 IEEE 2nd International Verification and Security Workshop (IVSW), 2017 Publication	1%
4	Submitted to Bharath University Student Paper	<1%
5	Konstantinos Karampidis, Ergina Kavallieratou, Giorgos Papadourakis. "A review of image	<1%