Proposed Approach to Enhanced Multimedia Information Security

1. Ankita Awasthi , 2. Amit Saxena

Abstract: The concept of image security and the word cryptography might be intimidating and complicated. The objective of the research is to design an idea that helps the user and the operations to achieve images security. Nowadays, information or image security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Steganography plays a significant role in the field of image hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. Most of the available steganography are mainly used only for single technique at a time but in this research, a new approach is propose to improve steganography technique. This approach is combining two techniques one is cryptography then followed by steganography. In cryptography, symmetric key cryptography are using to encrypt original image to produce cipher image and then this cipher image pass through steganography to produce final image . Performance of the propose approach is also analyzed and showing the expected results based on selected parameters. Expected results are proving the higher security and effectiveness in the performance.

Index terms: - *Steganography, Cryptography, Security, Encryption, Decryption, Internet, Image, Algorithm,*

1. Introduction

Maintaining privacy in our personal communications is something everyone desires. Cryptography is a means to achieve that privacy. It was invented for that very purpose. That makes cryptography a good idea, right? But cryptography, like most things, can be used for good or evil. And the debate over how to harness this powerful tool rages on as people on both sides see that there are no easy answers. In layman terms, cryptography or encryption is a process of converting readable or understandable information to a form that cannot be understood or read. This information, which cannot be read or understood, is often known to be ciphered information or encrypted data [10]. The process of recovering back the encrypted information is called decryption.
Since past times, governments and the military forces have used cryptography for transferring confidential information across. The very first use of cryptography can be seen in times of “Roman leader Julius Caesar where Julius Caesar” used a very basic method of encoding text. J”ulius Caesar” encrypted text messages and passed the same to his generals at war. The encryption method used by Julius came to be known as Caesar's Cipher or Shift Cipher and is the simplest and most widely used encoding method even today.
Cryptography by its own self suffice for encrypting data but a method known as Message Authentication Code (MAC) or Digital Signatures add to the protection level and integrity. Message Authentication is a piece of information that is used to authenticate encrypted data [10]. Digital Signatures are considered to be better than MAC and can be used to create different secret keys for sender and receiver. This way the information is more secure and authentic. Today, it might find atop-notch information security. A single slip up in encrypting the information properly can result into security breach. Encryption cannot be regarded as a perfect solution for our information security needs. Attack methods like traffic analysis, brute force or TEMPEST can still crack the encryption algorithm. Although a lot of algorithms I find today such as RSA and DES (Data Encryption Standard) are prominently very complex to break, but still it is possible to break them, even though very rarely [11]. Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images [11].
The Uses of Image Encryption: Encryption provides a much higher degree of security than anything else. One big area in which security is a concern is on the Internet. With the Internet holding close to an estimated 28 billion images and 2 billion web sites, it is easy to leave encrypted messages in a vast number of images as a security precaution. These encrypted messages can be used in various different means and methods.

One use of image encryption is to protect an image from it being downloaded by an anonymous user. Encrypting the image will lock the image to the designated website to prevent unauthorized downloading. For example, if a particular website has a certain image which is unique to that website and the creator does not wish other people to download that image, the creator will encrypt the image to avoid right clicking, downloading, and saving the image. Any random user can easily download a non-encrypted image, as opposed to an encrypted image, by right clicking. Image encryption also prevents bandwidth theft and unauthorized linking. With image encryption, an image can only be viewed from a registered website [12]. Images can even be safe from the web-master himself, without illegal scaling or resizing the image itself. The government also uses image encryption. They would use this for secure handling of intelligence data and intelligence activities. For civilians, image encryption can also be used for secure corporate communications and secure banking transactions. The medical field is another industry that uses image encryption. These encrypted images hold and store patient information. Rather than having a patient’s information in a thick folder of paperwork, the information is embedded into the patient’s x-ray image[12]. Embedding extra information into an image using encryption is an effective method for image integrity in tele-mammography. Image encryption not only helps regular civilians but it can also be used for bad intentions. For example, terror groups such as the Hamas, Hezbullah and Al-Qaida use uncrackable encryption to communicate about their criminal intentions without fear of outside intrusion, such as a government agency. There are two kinds of encryption, wherein, data is encrypted into an image and hidden from the public eye. Data encryption requires secret passwords and codes to view the image or hidden message. The second kind of encryption is an open key encryption which mainly prevents pretending, tampering and negation of the image itself, rather than encrypting it with data, it encrypts the image it self [13].

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means “covered writing.” It includes a vast array of secret communications methods that conceal the message’s very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum

communications. Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganography methods wills not [9]. The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication [3]. In modern approach, depending on the nature of cover object, steganography can be divided into five types [9]:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

2. RELATED WORK

Security, the most common word uttered by any user, any device, any peripheral since past two centuries. Protection from malicious sources has become a part of the invention or the discovery cycle. Myriad methods of protection are used ranging from a simple authentication password to most cryptography algorithms for protecting the extreme sensitive or confidential data. In [1] presented approach of steganography with cryptography which is using Cipher Block Chaining (CBC) mode for encryption to image by considering three different traversing path (Horizontal, Vertical and Diagonal). In this approach one simple Raster Scan has been employed to scramble the confidential Image called Horizontal Image Scrambling (HIS). Method two is a variant of method one called Vertical Image Scrambling (VIS), here traversing path would be top to bottom left to Right. Third approach employs diagonal traversing path called Diagonal Image Scrambling (DIS). Later standard Image Steganography has been used to send these Scrambled Images in an unnoticeable manner. In [2] an approach presented based on secrete sharing concept. This refers to a method of distributing a secret among a group of participants, each of whom is allocated with a share of the secret. The participant's shares are used to reconstruct the secret. Single individual participants share is of no use. The reversible image sharing approach and threshold schemes are suggested to achieve the secret image sharing for color full image. The secret color full image pixels will be transformed to m-ary notational system. The reversible polynomial function will be generated using (t-1) digits of secret color image pixels. Secret shares are generated with the help of reversible polynomial function and the participant's numerical key. The secret image and the cover image is embedded together to construct a stego image. The reversible image sharing process is used to reconstruct the secret image and cover image. The secret is obtained by the lagrange's formula generated from the sufficient secret shares. Quantization process is applied to improve the quality of the cover image. In [3] presents a novel from Greek, literally means "covered writing." It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganography methods wills not [9]. The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication [3]. In modern approach, depending on the nature of cover object, steganography can be divided into five types [9]:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

3. RELATED WORK

Security, the most common word uttered by any user, any device, any peripheral since past two centuries. Protection from malicious sources has become a part of the invention or the discovery cycle. Myriad methods of protection are used ranging from a simple authentication password to most cryptography algorithms for protecting the extreme sensitive or confidential data. In [1] presented approach of steganography with cryptography which is using Cipher Block Chaining (CBC) mode for encryption to image by considering three different traversing path (Horizontal, Vertical and Diagonal). In this approach one simple Raster Scan has been employed to scramble the confidential Image called Horizontal Image Scrambling (HIS). Method two is a variant of method one called Vertical Image Scrambling (VIS), here traversing path would be top to bottom left to Right. Third approach employs diagonal traversing path called Diagonal Image Scrambling (DIS). Later standard Image Steganography has been used to send these Scrambled Images in an unnoticeable manner. In [2] an approach presented based on secrete sharing concept. This refers to a method of distributing a secret among a group of participants, each of whom is allocated with a share of the secret. The participant's shares are used to reconstruct the secret. Single individual participants share is of no use. The reversible image sharing approach and threshold schemes are suggested to achieve the secret image sharing for color full image. The secret color full image pixels will be transformed to m-ary notational system. The reversible polynomial function will be generated using (t-1) digits of secret color image pixels. Secret shares are generated with the help of reversible polynomial function and the participant's numerical key. The secret image and the cover image is embedded together to construct a stego image. The reversible image sharing process is used to reconstruct the secret image and cover image. The secret is obtained by the lagrange's formula generated from the sufficient secret shares. Quantization process is applied to improve the quality of the cover image. In [3] presents a novel steganography technique for image which is based on Huffman Encoding. Two 8 bit gray image of size K X T and I X J are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/ before embedding and each bit of Huffman code of secret image/ is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image becomes standalone information to the receiver. In [4] presents a novel technique for Image steganography which is based on LSB using X-box mapping where authors used several Xboxes having unique data. The embedding part is done by this standard steganography algorithm where authors used four unique X-boxes with sixteen different values (represented by 4-bits) and each value is mapped to the four LSBs of the cover image.
The growth of high speed computer networks and that of the Internet, in particular, has increased the ease of Information Communication. Ironically, the cause for the development is also of the apprehension - use of digital formatted data. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. But this type advancement in the field of data communication in other sense has hiked the fear of getting the data snooped at the time of sending it from the sender to the receiver. So, Information Security is becoming an inseparable part of Data Communication. In order to address this Information Security Steganography plays an important role. Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. In [5] a review of the steganography techniques presented as a literature study. Various steganography techniques for image have been proposed. In this paper, we investigate steganography techniques and steganalysis techniques. We state a set of criteria to analyze and evaluate the strengths and weaknesses of the presented techniques. The least-

significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image with high capacity, while it is detectable by statistical analysis such as RS and Chi-square analyses. This paper has proposed a novel LSB image steganography algorithm that can effectively resist image steganalysis based on statistical analysis.

In [6] focused on two methods with suggested technique known as metamorphic cryptography. In this technique the message is transformed as a cipher image with the help of a key, scrambled with another image by using standard steganography technique by converting it into an intermediate text and finally transformed once again into an image.

As we know that the complexity of cryptography does not allow many user to actually understand the motivations and therefore available for practicing security cryptography. Cryptography process seeks to distribute an estimation of basic cryptographic primitives across a number of confluences in order to reduce security assumptions on individual nodes, which establish a level of fault-tolerance opposing to the node alteration. In a progressively networked and distributed communications environment, there are more and more useful situations where the ability to distribute a computation between a number of unlike network intersections is needed. The reason back to the efficiency (separate nodes perform distinct tasks), fault-tolerance (if some nodes are unavailable then others can perform the task) and security (the trust required to perform the task is shared between nodes) that order differently. Hence, [7] describe and review the different research that has done toward text encryption and description in the block cipher. Moreover, [7] suggests a cryptography model in the block cipher. In [8] expressive a novel algorithm of data hiding using cryptography named as ASK algorithm. Sensitive data is hided in a color image using cryptography. This shows how data can be send using a color image without ignorance of third party. Algorithm describes a method for vanishing data in a color image.

4. PROPOPSED WORK

In this proposed concept steganography works on the innovative idea of taking the consecutive or encrypted pixel bits of an confidential image and collectively worked and modified with logic, thereby leading to a complete set of new of pixel, which is a typical from the original bits. The detailed description is shown in Figure 1 and figure 2. A further complication could be added to the malignant attacker, by incorporating the proposed encryption method for image, by which the plain pixel bits is monumentally Scrambled to form the encrypted image, thereby making the data transfer very secure. A further addition of a key in the process makes the image tight/closed from any external agency. Later this encrypted confidential image has been embedded in the chosen cover image to form the stego image as shown in Figure 1.

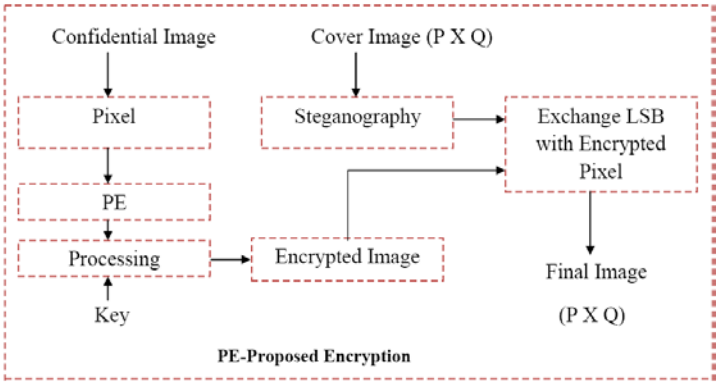

Figure 1: Flow Chart of Proposed Concept at One End (Encryption)

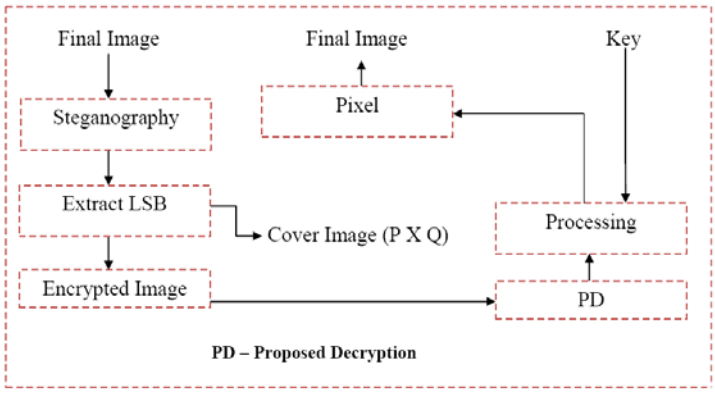

Figure 2: Flow Chart of Proposed Concept at another End (Decryption)

5. EXPECTED RESULTS AND CONCLUSION

During Performance evolution of the proposed concept we have selected some parameters which is following

- PSNR
- Execution Time
- Throughput
- Entropy
- Histogram

Expected results of the proposed concept are shown in table 1. This table show proposed concept performance based on selected parameters.

Table 1: Performance Observation of Proposed Concept

Parameters	Proposed Concept
PSNR	GOOD
T	HIGH
TP	HIGH
Entropy	HIGH
Histogram	GOOD

Conclusion: Its already known that destroy confidential image through encryption is completely distorted or unclear, the encrypted image as an intermediate output i.e. the image encryption can be extra modified with the help of the key in picturing a more aesthetic image for the hacker which when deeply checked will not leave a single trace of the randomization that has been introduced to the image. The results have also affirmed our conclusions. In this paper we have proposed a novel image steganography concept will be based on Proposed encryption of the image followed by the standard steganography. The proposed concept will improves the security and the quality of the stego image and will better in comparison with other existing approach. According to the expected results, the stego images of our proposed concept will almost identical to the cover images and it will very difficult to differentiate between them. We will achieved 100% recovery of the secret image that means original and extracted secret images will be identical.

.

REFRENCES

[1] Rengarajan Amirtharajan\ Anushiadevi .R2, Meena .y2, Kalpana. y2 and John Bosco Balaguru "Seeable Visual But Not Sure of It" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[2] [5] L.Jani Anbarasi and S.Kannan "Secured Secret Color Image Sharing With Steganography" IEEE 2012

[3] RigDas and Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding" IEEE 2012

[4] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar "An Image Steganography Technique using X-Box Mapping" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[5] G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan "Steganography Using Edge A Adaptive Image" IEEE International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012

[6] Thomas Leontin Philjon. and Venkateshvara Rao. "Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011

[7] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana "A Competitive Study of Cryptography Techniques over Block Cipher" UKSim 13th IEEE International Conference on Modelling and Simulation 2011

[8] Abhishek Gupta, Sandeep Mahapatra and, Karanveer Singh " Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm" 2011 IEEE

[9] danah boyd and Alice Marwick "Social Steganography: Privacy in Networked Publics" ICA 2011

[10] William stallings, "Cryptography and Network Security:Principles & Practices", second edition.

[11] Introduction of cryptography by H. Delfs and H. Knebl springer verlag berlin Heidelberg 2007

[12] William Stallings "Cryptography and Network Security",3rd Edition, Prentice-Hall Inc., 2005.

[13] Bruce Shnier "Applied Cryptography Second Edition Protocols. Algorithms, and Source, and Source Code in C", John Wiley and Sons, Inc., 1996.

- *Ankita Awasthi is currently pursuing masters degree program in computer science and engineering in RGPV University, PH - 09424696199. E-mail: ankitaawasthi2010@gmail.com*
- *Amit Saxena is currently pursuing phd program in computer scienceand engineering E-mail: amit.saxena78@gmail.com*