A Hybrid Image Steganography using DES and LSB based Technique

Nutan Manwade[1], Ms. Swati Nigam[2]

[1]M. Tech. Student, Dept. of EC, [2]Asst. Professor, Dept. of EC
Sanghvi Institute of Management & Science, Indore
R.G.P.V. University, Bhopal (M.P.)

Abstract – The cryptography is a classical domain of research and security. The cryptography offers the methods and techniques to hide the data from the untrusted users and recover them when required. The cryptographic technique is works on the basis of some passwords or keys. These keys help to make data more secure; according to the nature of keys the methods can be symmetric or asymmetric. But these techniques are traditional thus the attackers are break them using the different kinds of attack deployments. Therefore the cryptographic techniques are needed to be update with time.The proposed work is dedicated to investigate about the cryptographic techniques. In addition of that tried to develop a complex and secure method for securing the digital data. Therefore the proposed technique incorporates two traditional techniques to design secure image cryptographic technique. The proposed technique involves the DES based traditional cryptographic technique and the LSB based image stegnographic technique to secure the image data from outside intruders and attackers. To hide the data of the image a key image is also used with the proposed technique. By which the target image is encapsulated in the key image. The final cipher of the proposed technique is complex and not compromises with the quality of data during the decryption of image data.The implementation of the proposed technique is provided with the help of MATLAB technology. Additionally the performance of the proposed work is evaluated in terms of space and time complexity. Finally to justify the outcomes of the proposed technique a traditional approach is compared with the proposed technique with the similar performance factors. According to the obtained experimental results the proposed technique out perform as compared to traditional methods. Thus the proposed technique is enhance and adoptable for secure data in different applications.

Keywords: Image security, performance analysis, image cryptography, steganography, digital image processing.

I. INTRODUCTION

As Internet become more and more accessible now in these days. Therefore the data security is becoming more important research issues. Cryptography is used to secure e-mails, credit or debit card information, and other kinds of application data. The art of preserving data using cryptography by transforming it is called encryption. Into an unreadable format called cipher text. Additionally only the person who knows a secret key can decipher or decrypt into original message. But sometimes encipher messages can broke by attackers. This process is called cryptanalysis, or code-breaking. But modern cryptographic techniques are sometimes unbreakable. Cryptography systems can be broadly classified two broad categories. Symmetric-key technique usage a single key that is shared between both (sender and receiver), and Public-key cry Two keys usage cryptography, a public key known to everyone and a private key that only recipient of messages knows [1].

Now in these days, most of the applications are becomes online. Online applications help to provide various services at door steps in addition of that, due to this the service can be accessible at any point of time, and therefore demands of these applications are rapidly growing. In this context the user's confidential data and private information travelling in network. Most of the time that is used to represent the publically accessible networks thus the data is transmitted from secure environment to an untrusted or unsecured environment. In addition of that, the attackers become more equipped and technologically sound additionally they update self-time to time. Therefore the traditional approaches of information security become less effective and using the crypto-analysis the data is recovered by attacker. Thus to provide high secure data exchange a new kind of mathematical model is required by which the traditional data security schemes are improved.

By the motivation of secure data communication the proposed work is intended to investigate about the available techniques of cryptographic security. Among them the image cryptography is selected as initial objective of the work. In addition of that a design of a secure and efficient technique of file steganography is also proposed to develop. The proposed method involve the steganography technique and the traditional DES based cryptography to provide more secure data hiding technique over the traditional one. Therefore the proposed technique first include the image or input data which is required to hide in addition of that the technique also required a key image in which the image is going to hide. To hide image to other image the LSB (least significant bits) of the key image is used.

II. PROPOSED WORK

The proposed technique of image steganography is demonstrated and explained in this section. To understand the core concept of the proposed methodology the figure 1 and figure 2 helps.

A. Encryption process

The encryption process is demonstrated using the figure 1. In this process first the input image is produced for hiding them in a key image. Therefore the original image bits are shifted at the right and the new image data is created for 4bit density. In further the key image is produced to the system, this key image is XORed with the 4bit image. The outcome of this stage is now processed using the DES (Data Encryption Standard).

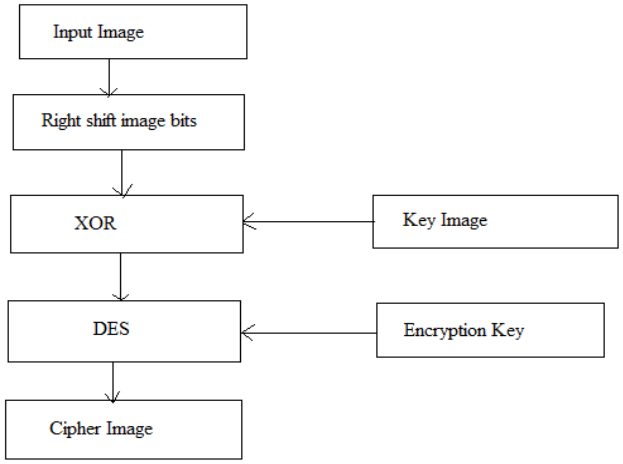

Figure 1 encryption process

Thus with the image data which is XORed with the input image is produced to DES algorithm with a 64 bit key. By using the DES encryption a new cipher text is appeared. This data is further used for transmission.

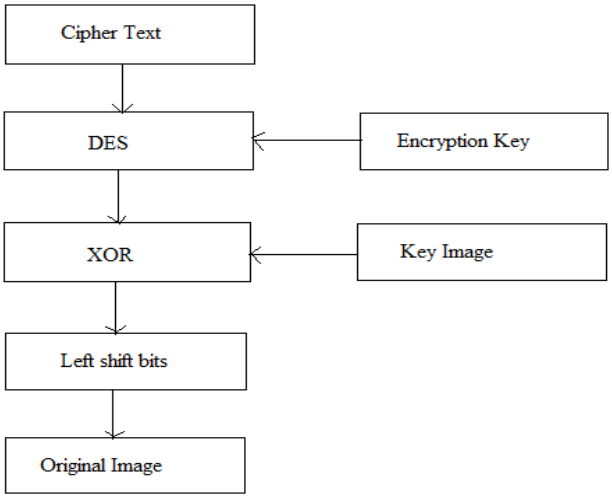

Figure 2 decryption technique

B. Decryption process

The proposed algorithm's decryption process is demonstrated using the figure 2. In this process the cipher text received from the sender is produced as input to the system. Now with the similar key and input cipher text the DES algorithm processes the data. The outcome of this process is now given to the input into an XOR pass. In this phase the key image and DES algorithm's output is consumed and new image data is prepared. That is not the complete information which is required, thus the data is processed with the left shift operator. The left shift technique produces the complete image. The complete image is the actual image which is transmitted by sender.

C. Proposed Algorithm

The last section provides the understanding about the processes involved in the proposed cryptographic technique. This section provides the summarized steps of the process for both the required operations.

Input: image to hide I_h, 64 bit key K_e, key image I_k Output: cipher image C
Process: I = readImage(I_h) $I_{Rh} = RightShift(I)$ $I_{xor} = I_{Rh} \oplus I_k$ $C = DES.encrypt(I_{xor}, K_e)$ Return C

Table 1 proposed encryption

In the similar manner the proposed decryption algorithm is works to generate the original image.

Input: cipher image C, 64 bit key K_e, key image I_k Output: image hidden I_h
Process: $C_i = ReadCipher(C)$ $I_{xor} = DES.Decrypt(C_i, K_e)$ $I_{Rh} = I_{xor} \oplus I_k$ $I = leftShift(I_{Rh})$ Return I

Table 2 proposed decryption

III. RESULTS ANALYSIS

After successfully implementation of the proposed image cryptographic technique, performance of proposed algorithm and traditional cryptographic algorithm is

evaluated and compared. The performance comparison of the implemented techniques is given using the below given parameters.

A. Encryption time

The amount of time required to encrypt data using selected algorithm is known as encryption time. The comparative encryption time of both algorithms for cryptography is using given figure 3. In this diagram the X axis shows the file size (in terms of KB-kilobytes) of images used for experiments and the Y axis shows the amount of time consumed for encryption in terms of seconds.

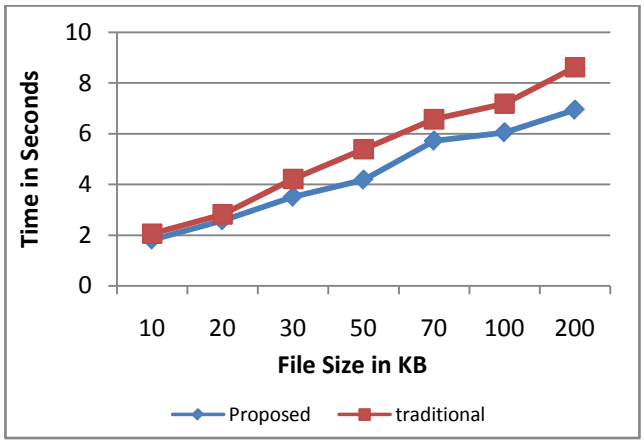

Figure 3 Time consumption in encryption

According to the performance of the traditional algorithm (represented using red line) consumes large time as compared to the proposed technique (given using blue line). Additionally with increasing size of data the time consumption is increase of traditional technique more rapidly as compared to proposed method. Therefore the proposed technique is more efficient as compared to traditional technique.

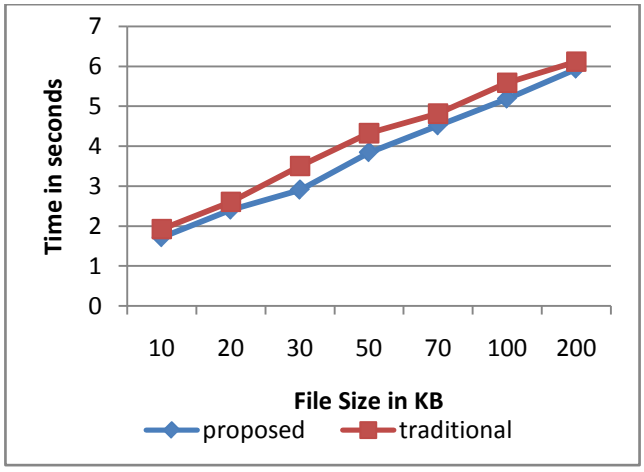

Figure 4 Time consumed in decryption

B. Decryption time

The amount of time required to recover the original image from the encipher image is termed as decryption time. The comparative time consumption of both the technique is represented using figure 4.In this diagram the performance of proposed technique is using the blue line and the red line shows the performance of traditional algorithm. For demonstration of the performance X axis contains the size of images on which experiments are performed that is given in terms of KB and Y axis shows the time in terms of seconds. The evaluated performance of the techniques shows the proposed algorithm is much efficient than the traditional method of cryptography in terms of time complication. Therefore the proposed technique is much adoptable as compared to the technique described in [1].

C. Encryption space complexity

The size of main memory required to achieve the implemented encryption algorithms is termed as encryption space complexity.Shows the comparative performance of the both algorithms for the space complexity of encryption in figure 5.

Figure 5 memory usage during encryption

For results confirmation the shows the different experiments performed with the system in x axis and the Y axis shows the memory consumption in terms of kilobytes during encryption.In order to show the performance of proposed algorithm the blue line is used and the red line is used to shows the performance of traditional algorithm. According to the given results most of the time the memory consumption in are much similar in both algorithm but sometimes that is increases unexpectedly. In addition the complexity of the space in algorithms are increases with the increasing size of experimental images. Therefore the proposed algorithm is much adoptable due to constant memory consumption.

D. Decryption space complexity

The memory consumed during the decipher or recovery of original algorithm is termed here as the decryption space complexity. The comparative results of the space complexity is given using figure 6 in this diagram the amount of memory used is given in terms of kilobytes using Y axis and the X axis shows the different experiments performed with the system. The performance of the proposed algorithm is given here using blue line and the traditional system is represented using the red line. According to the given results the proposed cryptographic technique consumes less memory and in consistent manner as compared to the traditional algorithm. Thus proposed technique is much adoptable as compared to traditional technique.

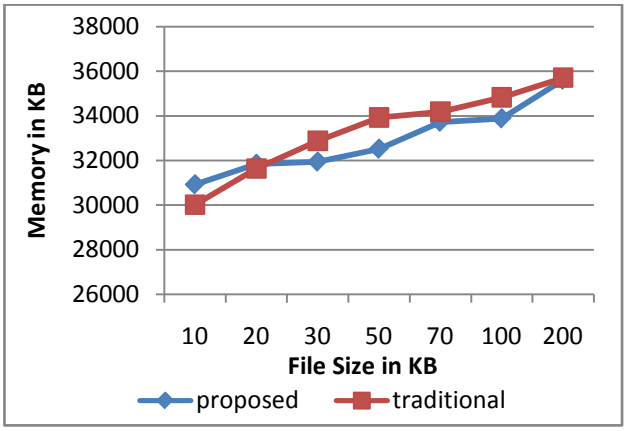

Figure 6 memory usage during decryption

E. PSNR (peak signal to noise ratio)

The peak signal-to-noise ratio measure the PSNR between two images. This ratio is often used to measure the quality between the original and a compressed image. Higher the PSNR means better the quality of the compressed or reconstructed image. The PSNR value can be calculated as:

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right)$$

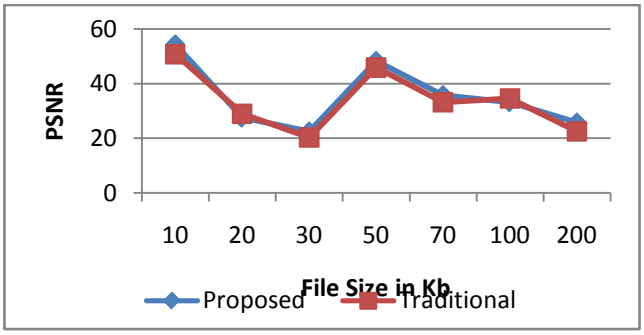

Figure 7 PSNR ratio

Peak signal to noise ratio of both the techniques for image stegnographic technique is given using figure 7. In this diagram the X axis shows the experimental file size and the Y axis shows the obtained PSNR ratio. The figure contains the red line to show the performance of the traditional approach and Y axis contains the performance of the proposed technique. The amount of computed PSNR is fluctuating with the image quality therefore that is not depends on the image size that is depends on the quality of image.

IV. CONCLUSIONS

The proposed work is intended to design and develop an enhanced technique of image cryptography. Therefore a LSB substitution based technique is proposed in this work. This chapter provides detailed conclusion of the work performed. In addition of that the future extension of the proposed work is also provided.

A. Conclusion

Security is a primary need of the digital data, different kinds of attacks and malicious programs can harm the data. In addition of that during the network transmission the data is also suspected to be stolen. Therefore different kinds of security techniques are implemented for enhancing the security of the digital data. In various security techniques the cryptography is popular and classical approach of data security. In this presented work the image cryptography is studied in detail and a new security technique using the steganography and data cryptography is proposed. The proposed cryptographic technique is hybrid technique which combines the efforts of both cryptography and steganography. Therefore the technique promises to provide more secure data exchange as compared to single technique implementation of image data security.

In the proposed technique two image are required first the image which is required to hide and the second image on which the data is required to be hide. The primary image is processed first and their image bits are first right shifted. This process is performed for 4 bit shift. After that the key image on which the data is going to be hiding is XOR with the new image data of 4 bit. Now the DES algorithm is implemented to improve the strength of the generated data cipher. The final outcome of the data is used for network transmission or other task. Similarly the decryption operation required to recover the original data, thus during the decryption the DES algorithm is used to decipher with a 64 bit key. In next the XOR is performed with the key image and finally the left shift operation is performed for producing the actual image. The implementation of the proposed cryptographic technique is performed using MATLAB tool and the performance of the implemented

system is computed. The performance of the implemented technique is compared with the traditional LSB based stegnographic technique. The comparative performance summary is given using the table 3.

Table 3 performance summary

S. No.	Parameters	Proposed	Traditional
1	Encryption time	Low	High
2	Decryption time	Low	High
3	Encryption space complexity	Low	High
4	Decryption space complexity	Low	High
5	PSNR	High	Low

According to the obtained results the proposed technique is found adoptable in resource consumption in addition of that using the PSNR values that is found the technique also not compromises with the image quality. Therefore the technique is adoptable and efficient for image cryptography and steganography.

B. Future work

In this presented work the key aim is to combine two different cryptographic techniques for data security, and enhance the safety in stegnographic method with less information consumption. That is accomplished successfully; in near future the proposed work is enhanced more for improving the cipher generation complexity enhancement to reduce the different kinds of attack effects.

V. REFERENCES

[1] VeerrajuGampala, SrilakshmiInuganti, SatishMuppidi, “Data Security in Cloud Computing with Elliptic Curve Cryptography”, IJSCE ISSN: 2231-2307, Volume-2, Issue-3, July 2012

[2] NadeemAkhtar, Shahbaaz Khan, PragatiJohri, “An Improved Inverted LSB Image Steganography”, 978-1-4799-2900-9/14/$31.00 ©2014 IEEE

[3] Dorothy Elizabeth Rob, ling Denning, “Cryptography and Data Security”, http://faculty.nps.edu/dedennin/publications/Denning-CryptographyDataSecurity.pdf

[4] Clerk Maxwell, “Digital image representation”, http://pippin.gimp.org/image_processing/chap_dir.htm

[5] Sian-Jheng Lin and Wei-Ho Chung, Member, IEEE, “A Probabilistic Model of Visual Cryptography Scheme With Dynamic Group”, IEEE Transactions On Information Forensics And Security, Vol.7, No.1, February 2012

[6] SankalpPrakash, MridulaPurohit, “Applied Hybrid Cryptography in Key-pair Generation of RSA implementation”, Applied Hybrid Cryptography in Key-pair Generation of RSA implementation IJICCT–JUL 2013;Vol 1,Issue 1;

[7] ChaitaliHaldankar, Sonia Kuwelkar, “Implementation Of AES And BLOWFISH Algorithm”, International Journal of Research in Engineering and Technology, Volume: 03 Special Issue: 03 | May-2014 | NCRIET-2014

[8] Norman D. Jorstad, Landgrave T. Smith Jr, “Cryptographic Algorithm Metrics”, Directorate for Freedom of Information and Security Review (OASD-PA) Department of Defense, January 1997

[9] E. Thambiraja, G. Ramesh, Dr. R. Umarani, “A Survey on Various Most Common Encryption Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012

[10] Mr. ROHITH S, Mr. VINAY G, “A Novel Two Stage Binary Image Security System Using (2, 2) Visual Cryptography Scheme”, IJCER | May-June 2012 | Vol. 2 | Issue No.3 |642-646

[11] Lahieb Mohammed Jawad and Ghazali Bin Sulong, “A Review of Color Image Encryption Techniques”, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 1, November 2013

[12] Wang Yu, “The LSB-based High Payload Information Steganography”, International Conference on Mechatronics, Electronic, Industrial and Control Engineering (MEIC 2015), 2015 The authors - Published by Atlantis Press

[13] NadeemAkhtar, PragatiJohri, Shahbaaz Khan, “Enhancing the Security and Quality of LSB based Image Steganography”, 5th International Conference on Computational Intelligence and Communication Networks, 978-0-7695-5069-5/13, 2013 IEEE

[14] MamtaJuneja and Parvinder Singh Sandhu, “Improved LSB based Steganography Techniques for Color Images in Spatial Domain”, International Journal of Network Security, Vol.16, No.6, PP.452-462, Nov. 2014

[15] P. Manimegalai, K.S.Gomathi, D.Ponniselvi, M.Santha, “The ImageStegnography and Steganalysis Based on Peak-Shaped Technique for MP3 Audio and Video”, IJCSMC, Vol. 3, Issue. 1, January 2014, pg.300 – 308

[16] Der-Chyuan Lou, Chen-Hao Hu, “LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis”, Information Sciences, 2011 Elsevier Inc.

[17] Ratnakirti Roy, AnirbanSarkar, SuvamoyChangder, "Chaos based Edge Adaptive Image Steganography", International Conference on Computational Intelligence: Modeling Techniques and Applications 2013

[18] ChandanMohapatra And ManjushaPandey, "A Review on current Methods and application of Digital image Steganography", International Journal of Multidisciplinary Approach and Studies, Volume 02, No.2, March – April, 2015

[19] Swati B. Singh, Ameya K. Naik, PragatiDwivedi, SwapnaPatil, "Analysis of data Hiding Algorithmsfor Image Security", International Journal of Students Research in Technology & Management Vol 3 (05), May 2015, ISSN 2321-2543, pg 350- 354

[20] HayfaaAbdulzahraAtee, Robiah Ahmad and NorlizaMohd Noor, "Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding", Middle-East Journal of Scientific Research 23 (7): 1450-1460, 2015

[21] Ashitosh S. Thorat, Prof. Dr. G. U. Kharat, "Steganography Based Navigation of Missile", International Journal of Advanced Research in Electronics and Communication Engineering Volume 4, Issue 6, June 2015