INTERNATIONAL JOURNAL OF SCIENTIFIC PROGRESS AND RESEARCH (IJSPR) ISSN: 2349-4689
Volume 21, Number 01, 2016

Text security using Cryptography and Image Steganography- A Review

Shivani Chauhan[1], Jyotsna[2], Shivali Katnoria[3], Amit Doegar[4]

[1, 2,3] *Dept. of Computer Science & Engineering, National Institute of Technical Teachers' Training and Research, Sector-26, Chandigarh 160019, India*
[4] *Assistant Professor, Dept. of Computer Science & Engineering, National Institute of Technical Teachers' Training and Research, Sector-26, Chandigarh 160019, India*
[1] shivanichauhan.1953@gmail.com [2] jyotsnabhumbla@gmail.com
[3] shivali_katnoria@yahoo.com [4] amit@nitttrchd.ac.in

Abstract- Information security has become necessity today because of increasing cyber crime. For security in communication system, there are many techniques which can be widely divided as two classes- Steganography and Cryptography. Steganography hides the existence of the secret message whereas cryptography transforms the secret message so that it cannot be understood by any unauthorised person. In this paper, various techniques combining steganography and cryptography are described. A comparative analysis has been done. This paper mainly focuses on the strength of combining cryptography and steganography.

Keywords - Steganography, cryptography, steganalysis

I. INTRODUCTION

In the last several years information security has become one of the major issues in communication system. With the passage of time, security requirements have been changing rapidly. Before the emergence of computer and network communications facilities, information security was primarily provided by physical and administrative means. But with introduction of computer, distributed systems and internet, automated tools are needed to protect information stored on the computer and measures are also required to secure the data transmission also. There are various forms of security attacks which demands high level of security. First is passive attack which has potential to know or exploits secret data from the communication system. The aim of attacker is to gain data that is transmitted. They are difficult to detect as they do not include any modification of message and messages are sent to receiver and received from receiver in a regular fashion without any hindrance. But measures are there to prevent their occurrence. For example-disclose of message contents (a telephone conversation etc.) and traffic analysis. Second is active attack which attempts to alter or affect system resources. They are relatively easy to detect, but difficult to prevent. For example- masquerade (when one entity pretends to be some other entity), replay (capture message and later replay), alteration of messages (a portion of message is modified), and denial of service (disruption of entire network or disable the network by overloading) [1]. Though security for information was an important issue and concern in ancient time also, but it has become a necessity today because of increasing cyber crime. Number of internet users is also increasing rapidly. For security in communication system, there are many techniques which can be widely divided as two classes- Steganography and Cryptography. Both the techniques are somewhat similar as they serve the same purpose of providing the security to information. But they are totally different in how they serve that purpose. Steganography is technique of hiding the existence of the secret information whereas cryptography is a technique of transforming the secret information so that it cannot be understood by the attacker. There are various types and techniques of steganography and cryptography.

II. CRYPTOGRAPHY

Man has used cryptography from many years in various forms for protecting the secret information. Around 1900 B.C., traces of cryptography can be found as a message carved on stone in Egypt. An earliest example was of Julius Caesar (that later came to known as Caesar cipher), who used a simple substitution method, by replacing each letter in message by another letter which is present some fixed number of place further down that alphabet. ATBASH was used by Hebrew scribes as a reversed alphabet simple solution cipher [2]. The idea of Caesar cipher was generalized by the Arabs to the

monoalphabetic substitution. With the advancements in technology, cryptography needed to be stronger so that communication can be safe. Cryptography is the study of converting the secret message into some unreadable form which is not understandable by the third person who is not supposed to know that information. It serves the aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication by the use of some mathematical techniques [3]. The word "Cryptography" has its origin from two Greek language words "kryptos" implying "hidden" and "graphein" implying "to write". Cryptography jumbles up the data or scrambles it using some algorithms [4]. Cryptography characterizes the technique and investigation of changing information into a succession of bits that shows up as irregular and pointless to a side onlooker or attacker. It is used to keep the message secret. The various approaches to implement security can beno security (do not implement security at all), security through obscurity (simply hide the existence of the system), host security (security is enforced for each host individually) and network security (to restrict network access to various hosts). The technique of breaking the encryption algorithm is known as cryptanalysis. It is the process of deciphering messages from non-readable format to readable format without knowing how they were encrypted.

The cryptographic technique consists of following components – Plaintext, Encryption, Ciphertext, Decryption and Key.

Plaintext - It refers to the secret information in the readable form which is to be transformed into non readable form.

Encryption - It refers to the technique of encoding the message or plaintext in to some other non readable form. The techniques used are known as encryption algorithms.

Ciphertext - Ciphertext is the output of encoding procedures that are applied to the plaintext. Ciphertext may be defined as the non readable form of the plaintext.

Decryption - It refers to the technique of decoding the ciphertext to get back the plaintext. It is the reverse of encryption. The techniques used are known as decryption algorithms.

Key - Encryption and decryption procedures are done by using a secret key to make the communication secure. It is the means by which it is assured that communication is in between authenticated parties.

III. STEGANOGRAPHY

There are various ancient examples of Steganography. It was first used in around 440 BC in the period of Golden Age at Greece. An ancient Greek record explains the Steganography. Demaratus practiced of liquefying wax tablet which were utilized for writing messages and then wrote a message in the underlying wood. The wax was then re-applied to the wood, giving the look of an unused tablet. The tablet was then transported without giving attention to anyone. It appeared blank and innocent to a common observer [5]. Herodotus, a Greek historian, tattooed a message on a worker's planed head and concealed under reproduced hair. Another example is French Resistance coded messages on the backs of couriers in invisible ink during world war ll. These are some of the traditional methods that were used for communicating secretly before the invention of digital means.

Steganography is the scientific discipline of inconspicuous communication by concealing useful secret data in some another media. It refers to the process of hiding the presence of the secret message. It is an art of covert writing. It does not keep the message secret but it provides the secrecy of the message. Steganography hides a secret message from the third party. It does not arouse an eavesdropper's attention. Dictionary.com states- "Steganography is hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message". The Steganography term is deduced from the Greek language words "*stegos*" implying "cover" and "*grafia*" implying "writing" and literally means "Cover writing". The algorithm by which secret message is embedded by the sender is known as embedding algorithm. The algorithm by which secret message is extracted at the receiver side is known as detector algorithm. Steganography should not be mistaken with cryptography because cryptography scrambles or encrypts the message to be sent so that it cannot be understood whereas steganography conceals the message into some other media so that its presence can be hidden. Any steganography technique must satisfy a no. of requirements- the integrity of the secret message which is embedded in stego-object must be accurate; the alteration in the stego-object should not be detected by the naked eye; choice of stego-object must be dependent on the size of secret message to be hidden and last but not the least we must always presume that malicious person knows that steganography is being used (that the stego-object is carrying some secret message). The Steganography systems consist of mainly three elements - Cover Object, Secret Message, Stego Object.

Cover Object - The cover objects are those in which we hide secret message. The cover object can be images, audio, videos, text.

Secret Message - The secret data is the data which we hide in the cover file or object to make its presence invisible. The secret message can be images, text messages etc.

Stego Object - The stego object is produced after hiding the secret information in cover image. After that stego object is transmitted and then at receiver side processing is done on stego object to retrieve message from it.

IV. COMPARISON OF STEGANOGRAPHY AND CRYPTOGRAPHY

Cryptography and steganography are similar in the purpose that they both provide information security. They are different in the sense how they provide that. Cryptography scrambles or jumbles the secret message so that it becomes meaningless or non-readable to the malicious person, whereas steganography conceals the presence of the secret message from the attacker. The result of cryptography is the cipher text whereas the result of steganography is the stego-object. Steganography refers to unknown message passing while cryptography refers to known message passing. Cryptography prevents a malicious person from detecting the contents of a communication while steganography prevents the detection of the presence of communication. In steganography, the structure of the secret message is not modified whereas in cryptography, the structure of the plaintext is modified. The steganography system is defeated if the attacker knows that steganography has been used and encoding system is known whereas cryptography system fails if the attacker is able to read the encrypted secret message.

V. COMBINATION OF STEGANOGRAPHY AND CRYPTOGRAPHY

For applications which require ultimate security in communication, cryptography and steganography can be used together. For adding multiple levels of security, it is beneficial to use both techniques together. This combination will enhance the requirements like security, capacity and robustness for secure data transmission. The combination of these two techniques provides better results with respect to security because cryptography secures the secret message by transforming it into non-readable form and steganography hides the presence of the secret message into some other medium. A vivid representation of the combination of cryptography together with steganography is shown in Fig.4. 1

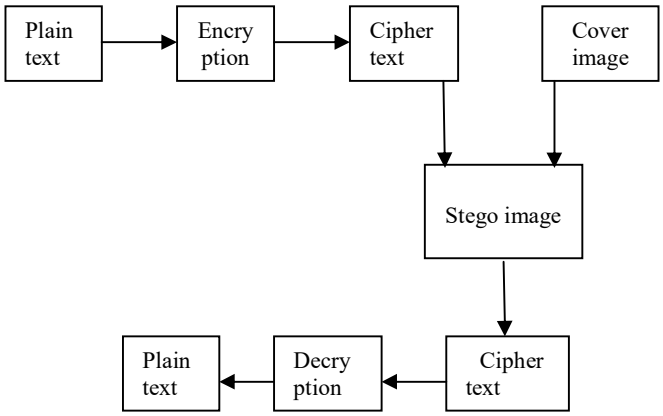

Fig.4.1 Combination of Cryptography and Steganography

In above figure, both the techniques are compounded by encrypting the plaintext first and then concealing it in the cover image using steganographic technique which results in stego-image. Then stego-image can be transmitted without giving clue of the secret information. If attacker somehow gets to know about the steganographic technique, he would still have to know the decoding key to decode the encrypted message.

VI. VARIOUS TECHNIQUES COMBINING CRYPTOGRAPHY AND STEGANOGRAPHY

Many researches have been done till now in the field of steganography. Many papers on the recent researches and developments in the field of steganography were studied. The literature survey basically provides a way to investigate for research and gives an idea of what has been done till date. A succinct review based on the study of these papers related to our pre-thesis is as follows.

Dr. Diwedi Samidha et al. [6] described several image steganography techniques in spatial domain. Along with existing techniques like LSB, layout management schemes and replacing only l's or only zero's, some more methods like replacing intermediate bit, raster scan principle, random scan principle, color based data hiding and shape based data hiding were also proposed. These new techniques were based on random selection of pixels for data hiding considering various characteristics of an image like physical location and intensity value of pixel, etc.

Vipul Sharma et al. [7] proposed two methods using both cryptography and steganography. In first method, image is secured by converting into text file using S-DES algorithm, secret key and then hiding it using steganography technique.

In second method, image is encrypted using S-DES and key image. They prevented steganalysis.

Amritpal Singh et al. [8] developed an improved method for image steganography using LSB technique. This worked by slicing the three planes of RGB image and then hiding the data into each plane based on color sensitivity by using LSB technique. It resulted in high embedding capacity and better image quality. Its PSNR value was better than previous steganographic methods.

Sourabh Chandra et al. [9] proposed a symmetric key cryptographic algorithm which is content based. This algorithm included binary addition operation for encrypting the plain text and circular shift operation and folding method for making the key secure. This algorithm posed a difficulty for opponent to decrypt the key and text.

Yogita Birdi et al. [10] proposed a method in steganography for secure communication. First, data is encrypted and then embedded using raster scan technique. This method made use of the Raster Scan Principle of displaying an image on CRT (Cathode Ray Tube) display. In this pixels have been hidden in the cover image in left to right and right to left manner. This made data extraction difficult for the opponent.

Bassam Jamil Mohd. et al. [11] developed a hardware design of LSB steganography technique in a cyclone II FPGA (Field Programmable Gate Array) of the Altera family. They proposed 2/3 LSB design which provided good visual quality of image and facilitated simple memory access.

Dr. Sudeep D. Thepade et al. [12] proposed Cosine wavelet transform, Walsh wavelet transform to be used for image steganography which were generated from Cosine, Walsh and Slant transforms respectively. They showed robustness to a good extent against attacks like cropping, brightness and darkness on stego than cosine transform. They provided balance of imperceptibility and robustness.

Ross J. Anderson et al. [13] clarified what is steganography and what purposes it serve. They provided its contrast with field of cryptography and also traffic security. They have described a number of attacks on information hiding schemes. It gave idea of practical value like the use of parity checks to enhance covertness, improve efficiency and give public key steganography. They showed that public key steganography is sometimes possible in presence of active warden.

Fabien A.P. Peticolas et al. [14] provided overview of the field of information hiding, particularly steganography. They described various steganographic techniques, a number of attacks on information hiding systems, limitations of information hiding systems and StirMark tool for robustness testing of image watermarking.

Pria Bharti et al. [15] proposed a method of data hiding by first encrypting the text and then embedding 4 bits information in a 4×4 block of pixel which changes very less pixel on average. This method was efficient for small data and for those images whose pixels are spread homogeneously. This method improved the quality of the stego image.

M. Radhika Mani et al. [16] proposed a method which relies on pattern based image steganography. In this sender could insert the secret message into hierarchically divided sub segments. In first stage, isolated the cover picture into 25x25 non coincided windows. Then after that, separated every window into 5x5 sub segments. At that point sub segment was chosen taking into account design ‘Z’ from among them. In second level, pixels were chosen based on pattern ‘a’ within each selected 5x5 sub sections. At last, 1 bit LSB method was applied in the selected pixels for embedding the secret message. This method demonstrated very good perceptual transparency and is easy to implement. It provided security from intruders. The method was efficient with respect to MSE, MAE, RMSE, PSNR and SNR.

R. Nivedhitha et al. [17] proposed a new technique by combining cryptography and steganography by encrypting the secret image with DES algorithm using key image and then hiding the secret encrypted picture into the cover picture utilizing LSB technique. The secret image could be decrypted using the same key image. This method was efficient for secret communication.

Pye Pye Aung et al. [18] provided a new method by combining AES algorithm for encrypting the secret message and then encrypted message was concealed in the DCT of an image by using a part of encrypted message as key. It produced efficient robust stego-image that poses difficulty in front of attacker to retrieve the secret message.

Nadeem Akhtar et al. [19] proposed two methods of bit inversion and improved plain LSB technique. In contrast with plain LSB technique, less number of pixels was modified as just those LSB’s of pixels of cover picture were reversed which happened with a specific pattern. It became hard for the opponent to recover the secret message bits as some of LSB’s have been inverted. This method also improves the security, image quality and PSNR value.

Kamaldeep Joshi et al. [20] worked on steganography in spatial domain and proposed a new image steganography method LSB-S in combination with cryptography. First of all, secret message was encrypted with transposition Vernam cipher algorithm and then embedding was done using four LSB of the pixel and performing circular left shift operation and XOR operation. The data hiding capacity was improved to almost 100%. The results showed good PSNR and MSE value.

S. M. Masud Karim et al. [21] introduced a newly enhanced method for LSB image steganography to improve security level. This method utilizes a secret key to secure the secret data and conceal in the LSB of image. In this, secret information is stored in different positions that are in LSB of Green or Blue matrix of a particular pixel relying upon the mystery key. It provided better PSNR value and better security.

Md. Palash Uddin et al. [22] developed an efficient method for text steganography along with cryptography. They used DES algorithm for encrypting the text message. After that encrypted message was embedded into the cover text which was as ordinary as possible. Finally, an alphanumeric riddle was appended toward the end of the cover text with the goal that it would appear like a conventional content to any third person. This was a format based text steganography which included additional security in information exchange.

Shuting Xu et al. [23] proposed an effective LSB algorithm relying on classic k-means algorithm. In this secret message bits were split into groups known as clusters and then groups were allotted to substitute the LSB of every pixel. A function has been defined to compute the separation between the bits and the groups. The use of k-means led to optimized stego-image.

Sarita Poonia et al. [24] amplified steganography by combining it with cryptography and watermarking. They applied LSB technique during DCT on cover image. Pretty Good Privacy (PGP) was used for encryption and decryption and digital watermarking was used to signify ownership and source authentication. This method provided very little distortion in the image.

Souvik Roy et al. [25] centred on safeguarding customer data during online shopping in E-commerce market. They presented a new approach with the combination of text based steganography and visual cryptography for giving just constrained information that is essential for fund exchange throughout internet shopping. This method minimized information sharing between online merchant and consumer forbidding wrong use of information at seller side while enabling successful fund transfer.

Nadeem Akhtar et al. [26] improved the robustness of steganography by using RC4 algorithm to achieve randomness in concealing message picture bits into cover picture pixels using a shared key. Bit inversion was also used to provide multi layer of protection as it will misguide the steganalysis process. This method improved security, image quality and robustness.

Pallavi Das et al. [27] proposed method for hiding multiple secret images of 8 bits in a single 24-bit cover image using LSB substitution based image steganography. Secret images were encrypted using Arnold transform before hiding. This method enhanced data hiding capacity highly while keeping the visual quality of the image satisfactory.

Sreeparna Chakrabarti et al. [28] developed a novel approach of image steganography to transmit the secret message securely. Firstly, encryption of secret message was done using secret key and after that encrypted secret message was hidden into the cover picture. This method provided two levels of stronger security.

Shahzad Alam et al. [29] objective was to raise the data hiding capacity and enhance the image quality. They proposed two approaches - first is 3-3-2 LSB approach without any restriction on the type of image used and the other is 4-4-4 LSB approach with limitations on type of image used. They concluded that in this work if size of data increases in bytes the PSNR value decreases and MSE increases.

Neil F. Johnson et al. [30] described steganography, image files and file compression methods. They explained a number of image steganographic approaches like LSB, masking and filtering etc. They also explored steganographic tools like S-Tools, stegoDos etc.

Krupi Patel et al. [31] developed an algorithm for binary image steganography in transform domain to hide a secret image along with cryptography to hike the level of security. They performed some operations like array padding and scrambling etc. on secret image and some pre-processing like normalization and DWT on the cover image and then fused both the images. At last inverse DWT and denormalization was performed to get the stego-image. The PSNR value obtained was high.

Santhoshi Bhatt et al. [32] combined image steganography using LSB technique and visible watermarking. They exploited those regions of image, also called as, which are unvarying to attacks. Scale Invariant feature Transform was used to find patches. They inserted watermarks in these patches as they are very stable and resistant to attacks. Results showed robustness against geometric distortion attacks and signal processing attacks.

Obaidah A. Rawashdeh et al. [33] proposed a new approach with a combination of image steganography and encryption. For choosing the key to encrypt the message primitive roots of prime numbers were used. Pixels to conceal the data were selected randomly using randomization characteristics of exponentiation of the primitive root numbers. The technique achieved high security and satisfactory level of image quality.

Saket Kumar et al. [34] presented image steganography to hide an image on multiple frae video using frame decomposition. LSB technique was used to hide the data. Password protection was also used to provide security to video. The watermarked image resisted different attacks and

data could be retrieved as it is. Each video frame was watermarked with color map of RGB image with encryption of password. Exact RGB image was retrieved after decoding with the help of color map.

Madhusudan Mishra et al. [35] introduced a new technique by combining public key cryptography and digital image steganography. They used RSA algorithm for encrypting the secret message and F5 steganographic method was utilized to conceal the encrypted message. Data embedding was done into randomly chosen DCT coefficients by F5 algorithm. The stego image and cover image were perceptually similar and the stego images were robust against image processing distortions.

Ashitosh S. Thorat et al. [36] designed a system for military application. This approach was developed to protect the data from unauthorized access. LSB technique was used to conceal the secret data randomly in the cover object. A stego-key was also applied to the system while embedding the message. Any type of cover file could be used such as image, audio or video files.

Shamim Ahmed Laskar et al. [37] proposed a novel steganographic approach that used LSB insertion to conceal the secret data in the LSB of red plane only. This approach focussed on providing security. This method provided efficient data hiding by HVS perceptual results and statistical image properties.

Ishant Premi et al. [38] proposed a secure technique for image steganography. The secret message was encrypted first with the secret key and then the encrypted message was concealed in random bits of cover image. They used XORing method instead of simply replacing the data. The values of MSE, PSNR and correlation were found to be satisfactory.

Shahzad Alam et al. [39] proposed a secure image steganography scheme. In this edge image was obtained by using canny edge detection from gray scale image. This method utilised random LSB steganography method. This method proved to be successful in gaining high payload and good quality stego image. It was also found to be robust to attacks and message could not be retrieved without knowing the key.

Rina Mishra et al. [40] proposed a new technique in which firstly the compression of secret data was done using LZW algorithm to reduce its size. Secondly, the compressed data was encrypted using RSA algorithm. Finally, edge of the image was obtained by canny edge detector and compressed encrypted message was embedded on the locations which were determined by the help of hash function. The strength of this technique was huge data hiding capacity and least distortion in stego image.

Rupali Bhardwaj et al. [41] proposed technique to provide two levels of security. In this method, secret data was jumbled in a random order generated by 2D Arnold Cat Map and then the encrypted message was hidden in cover image using basic LSB method. The values of PSNR and MSE were better than the simple LSB method.

Sumit Laha et al. [42] proposed an embedding algorithm to conceal secret data. After embedding using LSB method, the stego image quality was optimized by Genetic Algorithm. The process to extract the data required the cover image also. This method resulted in high PSNR value.

Gandharba Swain [43] proposed a new approach known as group of bits substitution(GBS). The basic idea was to substitute a group of bits in a pixel by another group of bits of same length. Some predefined conditions determine the number of bits selected for substitution. The maximum change in a pixel was not more than 2 bits per pixel. There were two schemes- 1-bit per pixel (hides one bit per pixel) and 2-bit per pixel (hides two bit per pixel). Group length was made variable for different pixels to improve security. The PSNR of 2-bit GBS was highly improved than that of 2-bit GBS.

Vladimir Hajduk et al. [44] proposed an image steganographic method by embedding secret message in the form of Quick Response(QR) code into image. For QR code embedding DWT domain was used and AES was used to protect the embedding process. The QR code module size was also compressed before embedding. The PSNR value achieved was better than existing methods.

VII. CONCLUSION

This paper is a survey of various techniques combining cryptography and steganography. Some techniques of steganography provide security and some provides enhanced data hiding capacity. It is difficult to provide high class security with steganography only, so combination of cryptography and steganography is used to provide double tier security. Many algorithms have been proposed by combining cryptography and steganography. Cryptographic algorithm like DES and AES etc. are used with steganographic algorithms, but in these block cipher algorithms, block size remains same. Cryptographic algorithm having varied block size can be combined with steganographic algorithm. No single technique can be generalized for all types of security measures. Also conclude that PSNR value depends upon the amount of data to be hidden and cover image size.

VIII. REFERENCES

[1] W. Stallings, "Cryptography and Network Security: Principles and Practices, fourth edition", pp. 592, November 2005.

[2] A. J. Raphael and V. Sundaram, "Cryptography and steganography – A survey", International Journal of Computing Technology and Applications, vol. 2, no. 3, pp. 626–630, 2011.

[3] D. Bloisi and L. Iocchi, "Image Based Steganography and Cryptography", Rochester, N.Y., 1996.

[4] V. Sharma, "Two New Approaches for Image Steganography Using Cryptography", IEEE Third International Conference on Image Information Processing(ICIIP), pp. 202–207, 2015.

[5] A. Kumar and Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications, vol. 9, no. 7, pp. 19–23, November 2010.

[6] D. Samidha and D. Agrawa, "Random Image Steganography in Spatial Domain", IEEE International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System(ICEVENT), pp. 1–3, 2013.

[7] V. Sharma, "Two New Approaches for Image Steganography Using Cryptography", IEEE Third International Conference on Image Information Processing(ICIIP), pp. 202–207, 2015.

[8] A. Singh and H. Singh, "An Improved LSB Based Image Steganography Technique for RGB Color Images", IEEE International Conference on Electrical, Computer and Communication technologies, pp. 1-4, 2015.

[9] S. Chandra, B. Mandal, S. S. Alam, and S. Bhattacharyya, "Content Based Double Encryption Algorithm Using Symmetric Key Cryptography", Procedia computer Science International Conference on Recent Trends in Computing(ICRTC), vol. 57, pp. 1228–1234, 2015.

[10] Y. Birdi and Harjinder Singh, "Raster Scan Technique for Secure Communication in Steganography", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 4, no. 6, pp. 5174–5179, 2015.

[11] B. J. Mohd, S. Abed, T. Al-Hayajneh, and S. Alouneh, "FPGA hardware of the LSB Steganography Method", IEEE International Conference on Computer, Information and Telecommunication Systems(CITS), pp. 1–4, 2012.

[12] S. D. Thepade and S. S. Chavan, "Cosine, Walsh and Slant Wavelet Transforms for Robust Image Steganography", IEEE Tenth International Conference on Wireless and Optical Communication Networks(WOCN), pp. 1-5, 2013.

[13] R. J. Anderson and F. A. P. Peticolas, "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, vol. 16, no. 4, pp. 474–481, May 1998.

[14] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding - A Survey", Proceedings of the IEEE, Special issue on protection of multimedia content, vol. 87, no. 7, pp. 1062–1078, July 1999.

[15] P. Bharti and R. Soni, "A New Approach of Data Hiding in Images using Cryptography and Steganography", International Journal of Computer Applications, vol. 58, no. 18, pp. 1–4, 2012.

[16] M. R. Mani, V. Lalithya and P. S. Rekha, "An Innovative Approach for Pattern based Image Steganography", IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems(SPICES), pp. 1–4, 2015.

[17] R. Nivedhitha and T. Meyyappan, "Image Security Using Steganography And Cryptographic Techniques", International Journal of Engineering Trends and Technology, vol. 3, pp. 366–371, 2012.

[18] P. P. Aung and T. M. Naing, "A Novel Secure Combination Technique of Steganography and Cryptography", International Journal of Information Technology, Modeling and Computing(IJITMC), vol. 2, no. 1, pp. 55–62, February 2014.

[19] N. Akhtar, S. Khan, and P. Johri, "An Improved Inverted LSB Image Steganography", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques(ICICT), pp. 749–755, 2014.

[20] K. Joshi and R. Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", IEEE Third International Conference on Image Information Processing(ICIIP), pp. 86–90, 2015.

[21] S. M. M. Karim, M. S. Rahman, and M. I. Hossain, "A New Approach for LSB based Image Steganography using Secret Key", IEEE 14th International Conference on Computer and Information Technology(ICCIT), pp. 286–291, 2011.

[22] M. P. Uddin, M. Saha, S. J. Ferdousi, M. I. Afjal, and M. A. Marjan, "Developing an Efficient Solution to Information Hiding through Text Steganography along with Cryptography", IEEE 9th International Forum on Strategic Technology(IFOST), pp. 14–17, 2014.

[23] S. Xu and Shuhua Lai, "An Optimal Least Significant Bit Based Image Steganography Algorithm", 2014.

[24] S. Poonia, M. Nokhwal, and A. Shankar, "A Secure Image Based Steganography and Cryptography with

Watermarking", International Journal of Emerging Science and Engineering(IJESE), vol. 1, no. 8, pp. 66–70, June 2013.

[25] S. Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", IEEE Students' Conference on Electrical, Electronics and Computer Science(SCEECS), pp. 1-5, 2014.

[26] N. Akhtar, P. Johri, and S. Khan, "Enhancing the Security and Quality of LSB based Image Steganography", IEEE 5th International Conference on Computational Intelligence and Communication Networks, pp. 385–390, 2013.

[27] P. Das, S. C. Kushwaha, and M. Chakraborty, "Multiple Embedding secret key Image Steganography using LSB substitution and Arnold Transform", IEEE sponsored 2nd International Conference on Electronics and Communication System(ICECS), pp. 845–849, 2015

[28] S. Chakrabarti and D. Samanta, "A Novel Approach to Digital Image Steganography of Key-Based Encrypted Text", IEEE International Conference on Electricals, Electronics, Signals, Communication and Optimization(EESCO), pp. 1-6, 2015.

[29] S. Alam, S. M. Zakariya, and M. Q. Rafiq, "Analysis of Modified LSB Approaches of Hiding Information in Digital Images", IEEE 5th International Conference on Computational Intelligence and Communication Networks(CICN), pp. 280–285, 2013

[30] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer Society, vol. 31, no. 2, pp. 26 – 34, 1998.

[31] K. Patel and L. Ragha, "Binary image Steganography in wavelet domain", IEEE International Conference on Industrial Instrumentation and Control(ICIC), pp. 1635–1640, 2015.

[32] S. Bhatt, A. Ray, A. Ghosh, and A. Ray, "Image Steganography and Visible Watermarking using LSB Extraction Technique", IEEE sponsored 9th International Conference on Intelligent Systems and Control(ISCO), pp. 1-6, 2015.

[33] O. A. Rawashdeh and Dr. N. A. M. Al-Saiyed, "A Novel Approach for Integrating Image Steganography and Encryption", International Journal of Computer Technology and Applications(IJCTA), vol. 5, no. 6, pp. 1917–1923, 2014.

[34] S. Kumar, A. K. Yadav, A. Gupta and P. Kumar, "RGB image Steganography on Multiple Frame Video using LSB Technique", IEEE International Conference on Computer and Computational Sciences(ICCCS)", pp. 226-231, 2015.

[35] M. Mishra, G. Tiwari and A. K. Yadav, "Secret Communication using public key Steganography", IEEE International Conference on Recent Advances and Innovation in Engineering(ICRAIE), pp. 1-5, May 2014.

[36] A. S. Thorat and G. U. Kharat, "Steganography Based Navigation of Missile", International Journal of Advanced Research in Electronics and Communication Engineering(IJARECE), vol. 4, no. 6, pp. 1662–1665, June 2015.

[37] S. A. Laskar and K. Hemachandran, "Steganography based on Random Pixel Selection for Efficient Data hiding", International Journal of Computer Engineering and Technology(IJCET), vol. 4, no. 2, pp. 31–44, 2013.

[38] I. Premi and S. Kaur, "Random Scan Algorithm for Image Steganography in Scilab for Security Purposes", International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 12, pp. 8876–8879, December 2014.

[39] S. Alam, V. Kumar, W. A. Siddiqui and M. Ahmad, "Key Dependent Image Steganography Using Edge Detection", IEEE International Conference on Advanced Computing and Communication Technologies, pp. 85-88, 2014.

[40] R. Mishra, A. Mishra, and P. Bhanodiya, "An Edge Based Image Steganography with Compression and Encryption", IEEE International Conference on Computer, Communication and Control(IC4), pp. 1–4, 2015.

[41] R. Bhardwaj and D. Khanna, "Enhanced the Security of Image Steganography Through Image Encryption", Annual IEEE India Conference(INDICON), pp. 1–4, 2015.

[42] S. Laha and R. Roy, "An improved image steganography scheme with high visual image quality", IEEE International Conference on Computing, Communication and Security(ICCCS), pp. 1-6, 2015.

[43] G. Swain, "Digital Image Steganography using variable length group of bits substitution", Procedia Computer Science International Conference on Computational Modeling and Security(CMS), vol. 85, pp. 31-38, 2016.

[44] V. Hajduk, M. Broda, O. Kovac and D. Levicky, "Image Steganography using QR code and cryptography", IEEE 26th Conference Radioelectronika, pp. 350-353, 2016.