International Journal of Advance Research in Science and Engineering
Volume No. 10, Issue No. 07, July 2021
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Securing Images using Cryptography & Data Hiding Techniques

Supriya Mishra[1] Mr. Abhinandan Tripathi[2]

[1]M.Tech. Student [2]Assistant Professor

[1,2]Department of Computer Science & Engineering

[1,2]Buddha Institute of Technology, Gorakhpur, India

Abstract: Now a days there is several problem related to security, there is many platform where people mainly post there videos and photos for interaction to other people. Data security is becoming increasingly important along with the increase of digital form of communication on the internet. In this paper we use several algorithm technique for implements the security of images such as steganography method where we hide the image and text in cover and cryptography method for using security key and encryption of files. An improved LSB information hiding algorithm of color image using secret key is be proposed, combining information hiding and cryptography. The study modelled the system and implemented it to be tested to explore the relation between security, capacity and data dependency.

Keywords: Steganography, Metamorphic Cryptography, Cryptography, Keys.

I. Introduction:

Usually, we need to secure sensitive data that we store on personal computers such as e-mail messages, health information, family private pictures, bank information, and credit card information. Securing sensitive secret text in the personal computers (PC) has benefit of the capability to allow the PC available files to act as the private cover [1]. Nowadays information hiding as main means in some areas such as secure communications, protection of intellectual property rights and content authentication, has been widely studied and applied. In order to provide confidence and safety to the user to protect his information on a PC, we combine cryptography and steganography techniques, i.e. for hiding sensitive data, as presented earlier for hiding in images [2] but here utilizing image based steganography. Therefore, it is preferred to use another technique such as cryptography to encrypt the sensitive data before hiding it in the cover media. That will ensure that even if the embedded text is discovered, no one can know its content because it is encrypted [4]. Therefore, for higher security, we can take advantage of combining the two techniques to ensure that even for the very difficult security penetration; still the sensitive data are not harmed or used negatively. Steganography in general, is the science of concealing information through a certain process. In this work, we suggested and implemented the flexible two layers technique, i.e. cryptography and steganography, to benefit from both and give the best possible security dedicated for PC applications. The cryptography layer is using DES crypto algorithm assuming its security reputation and simplicity [5].The steganography layer is adopting the video based steganography due to its popular availability and personal favor in PCs [1]. This video based steganography is concealing the ciphered text in the least significant bit (LSB) [6] and trying to improve its capacity by increasing the number of hiding LSBs, similar to the principle idea in [7]. The structure of this paper is as follows. The following section, Section

2, presents brief literature review of related work and similar ideas that should be considered in this study. This related work section is describing several techniques using in another cover medium

type, i.e. text, image, audio and videos [2]. This work focuses on video based steganography where the imbedding is performed with the encrypted secret hidden in the cover object [3]. Cryptography, as the other layer within this security system, is mainly encrypting the secret plain text converting it to cipher text [1]. In our security system, the sensitive text data passes through the crypto layer followed by the steganography layer resulting the output file as stego-image.Figure-1 shows the main overview of the method using this two-layer techniques.

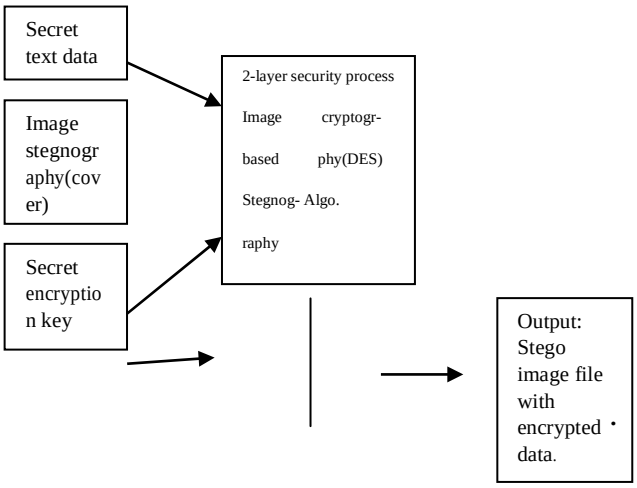

Figure 1: 2-layer techniques used for overall process

i. Cryptography:

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It is always assumed that a third party, often called adversary, can listen to the communication channel carrying such a message and accordingly by applying a cryptographic mechanism called encryption algorithm using a piece of information that is only know to the communicating parties and explicitly can acquire the message. Preventing such of data, non-alteration of data and so on. Cryptography is widely used today because of great security. The most desirable property of any image cryptography is to maximize the strength of the secret key in order not to be hacked and to be secured against detection by unauthorized parties. Encryption is a way to protect information from unwanted attacks by changing it into a form that cannot be recognized by any attackers. Data encryption is used for changing the data i.e. audio, text, and image, etc.By which it is unreadable, invisible or impenetrable during the transmission. So in order to recover the original data from the encrypt data we just use decryption method by which we receive original data called decryption.

Types of cryptography:

a. Symmetric key cryptosystems

All the classical cryptosystems that were developed before 1970 are an example of symmetric key cryptosystems. Besides that, most of the cryptosystems developed after 1970 are symmetric. Some of the very popular examples of modern symmetric key include:

AES (Advanced Encryption Standard) DES (Data Encryption Standard)

Symmetric key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of Cipher text. The secret is used for both encryption and decryption. The main problem in symmetric is that it has no capacity to handle large network of adversary from understanding the message is achieved unknown to the adversary. This piece of information is called the key of the encryption algorithm and the algorithm along with the key is called a cryptosystem. Cryptography provides a number of security properties to ensure the privacy communication. On the other hand, the symmetric key requires a smaller size for the same level of security as public key cryptosystems, thus, making the communication faster and memory required smaller.

b. Public key cryptosystems

In this type of cryptosystems, there are two separate keys: a public key, which is known publicly and the secret key, which is only known to the owner. This type of system is known as 'asymmetric' for the reason of using a different key for decryption and encryption (the public and private key). The data is encrypted by using some secret (public) key and only decrypted using the private key.

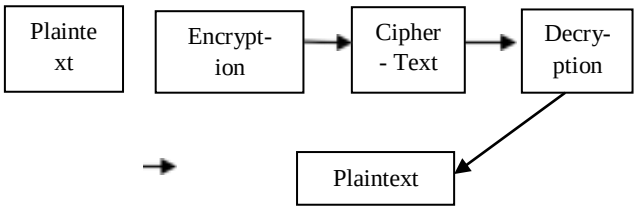

Figure 2: Cryptography Process

ii. Steganography

"Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by the cover message with the embedded cryptosystem. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present". In image steganography the information is hidden exclusively in images. The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to

communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the
slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. In size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

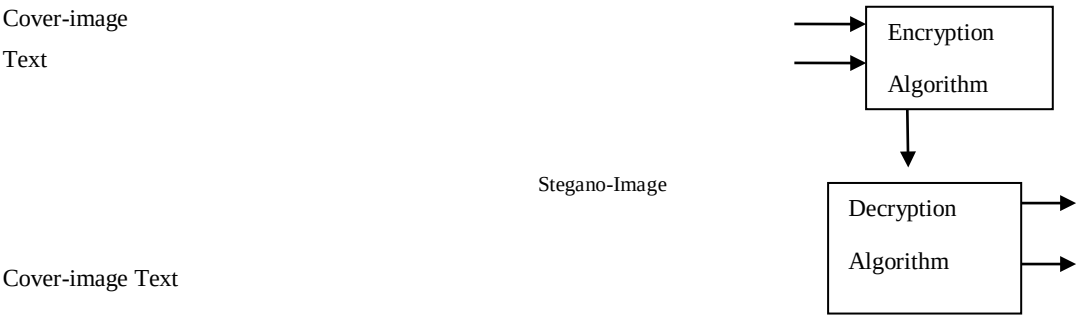

Figure 3: Steganography Process

Least Significant Bit:

Least significant bit (LSB) algorithm used in this paper is a spatial domain steganography in substitution method; the principle is to replace information in the least bit of cover image with confidential information. For 256 gray scale cover image, the gray scale value of each pixel can be used to represent 8-bit binary, taken out a certain bit of all pixels constitute a certain bit plane, for example, the least significant bit of all the pixels constituting the least significant bit plane. The higher the bit plane, the greater the contribution of the gray value, and the lowest bit plane is similar to random noise [3].

II. Related Work

In most of the papers proposing new algorithms for video encryption, the common idea is to act on a limited number of parts, those influencing more the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the reconstruction (that must be correct for the authorized users and obscure for the unauthorized ones) of the images at the receiver. These selected

data are encoded by using well known symmetric algorithms, like DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm), or by resorting to simple logic operations between the information data and a properly designed encryption key. The modern formulation of steganography is often given in terms of the prisoners' problem (Simmons, 1984; Kharrazi et al., 2004) where Alice and Bob are two inmates who wish to communicate in order to hatch an escape plan(2). Domenici Bloisi and Luca Iocchi

(2) proven that the presented ISC algorithm is both an effective steganographic method (they made a comparison with F5) as well as a theoretically unbreakable cryptographic one (ISC is an image based one-time pad). .(3)Yen and Guo suggested in [I3] to change the grey level of each pixel by means of an XOR or an XNOR logic operation with two prefixed keys: the operation and the key were selected on the basis of the values

outgoing a one- dimension chaotic system(4). The RSA standard is not used directly to encrypt/decrypt the data in the MPEG-I bit stream, because it requires a long processing time. This processing time is directly proportional to the size of the data to be encrypted. Ramadan J. Mustafa said that a DCT-based robust video steganographic method using BCH error correcting codes has been proposed. The steganography algorithm converts the video into frames; then, it divides each frame into Y, U, and V components. Prior to the embedding process, the secret message is encrypted and encoded using BCH codes. (9) Several researchers have addressed the problem of video steganography. In [4] a comparative analysis between Joint Picture Expert Group (JPEG) image stegano and Audio Video Interleaved (AVI) image stegano by quality and size was performed. The authors propose to increase the strength of the key by using UTF-32 encoding in the swapping algorithm and lossless stegano technique in the AVI file. However, payload capacity is low. Many techniques are found in the literature appropriate for PC security applications. This section reviews research that integrated the two Figure 1- Overview of the proposed 2-layer security system Nouf A. Al-Juaid, Adnan A. Gutub, Esam A. Khan10 techniques of cryptography and steganography utilizing video covers. Deshmukh et al. [8] introduced a hash- based LSB method for video steganography that conceals secret data or information within a video. Firstly, the location of the insertion in the LSB bit is determined using a hash function. Then, the secret text is concealed in the selected position of the LSB. In this paper, they applied the method to AVI files and measured the PSNR and MSE for comparison with the original video file. In contrast, Singh in [5] suggested a way to embed text in video files using LSB substitution. The embedding is done in a location in LSB bits according to equations noted in the paper. The advantage of this method is a simple and successful process for hiding secret messages more securely.

III. Proposed Model

In this paper, we suggested and implemented the flexible two layers technique, i.e. Cryptography and steganography, to benefit from both and given the best possible security dedicated for pc application. The cryptography layer is using DES CryptoAlgo. Assuming its security reputation and simplicity .The Steganography layer is adopting the image based stenography due to its popular availability and personal favour in Pcs.Now the beginning of the paper the first step is used to hide the image and text by steganography method. The process and explanation of steganography method is the practice of concealing a message within another message or a physical object. In computing/electronic contexts, a computer file,

message, image, or video is concealed file within another file, message image or video. These days, many examples of steganography involve embedding a secret piece of text inside of a picture. The process of steganography model is shown in figure

International Journal of Advance Research in Science and Engineering
Volume No. 10, Issue No. 07, July 2021
www.ijarse.com
IJARSE
ISSN 2319 - 8354

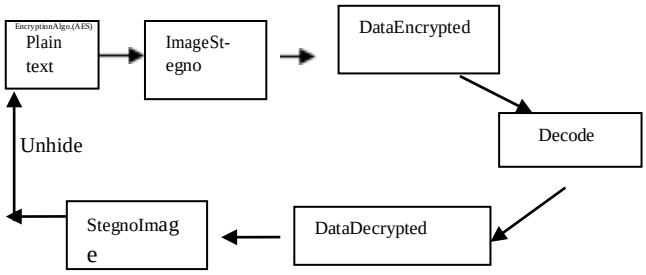

Figure 4: Crypto-Stegno Process

i. Image Based Steganography Systems:

The majority of today's steganographic systems uses images as cover media because people often transmit digital pictures over email and other Internet communication (e.g., eBay). Moreover, after digitalization, images contain the so-called quantization noise which provides space to embed data (Westfeld and Pfitzmann, 1999). In this article, we will concentrate only on images as carrier media. The modern formulation of steganography is often given in terms of the prisoners' problem (Simmons, 1984; Kharrazi et al., 2004) where Alice and Bob are two inmates who wish to communicate in order to hatch an escape plan. However, all communication between them is examined by the warden, Wendy, who will put them in solitary confinement at the slightest suspicion of covert communication. Specifically, in the general model for steganography, we have Alice (the sender) wishing to send a secret message M to Bob (the receiver): in order to do this, Alice chooses a cover image C. The steganographic algorithm identifies C's redundant bits (i.e., those that can be modified without arising Wendy's suspicion), then the embedding process creates a stego image S by replacing these redundant bits with data from M. S is transmitted over a public channel (monitored by Wendy) and is received by Bob only if Wendy has no suspicion on it. Once Bob recovers S, he can get M through the extracting process. The embedding process represents the critical task for a steganographic system since S must be as similar as possible to C for avoiding Wendy's intervention (Wendy acts for the eavesdropper). Least significant bit (LSB) insertion is a common and simple approach to embed information in a cover file: it overwrites the LSB of a pixel with an M's bit. If we choose a 24-bit image as cover, we can store 3 bits in each pixel. To the human eye, the resulting stego image will look identical to the cover image (Johnson and Jajodia, 1998). Unfortunately, modifying the cover image changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego image's statistical properties. In fact, the embedding of high-entropy data (often due to encryption) changes the histogram of colour frequencies in a predictable way (Provos and Honeyman, 2003; Westfield and Pfitzmann, 1999). Westfield (Westfield, 2001) proposed F5, an algorithm that does not overwrite LSB and preserves the stego image's statistical properties. Since standard steganographic systems do not provide strong message encryption, they recommend to encrypt M before embedding. Because of this, we have always to deal with a two- steps protocol: first we must cipher M (obtaining M') and then we can embed M' in C. In the next sections we will present a new all-inone method able to perform steganography providing strong encryption at the same time. Our method has been planned either to work with bit streams scattered over multiple images (in an online

way of functioning) or to work with still images; it yields random outputs, in order to make steganalysis more difficult and it can cipher M in a theoretically secure manner preserving the stego image's statistical properties. The simplicity of our method gives the possibility of using it in real-time applications such as mobile video communication.

ii. Distribution of DES key:

To guard against brute force attack, the DES key is changed periodically and transmitted to the receiver in an encrypted form. If a crypt-analyst manages to get one of these keys and to use it to attack the video, he will not be able to compromise the entire video. He will be able to decrypt only the frames encrypted with that key. The key is transmitted within the MPEG-I video bit stream in the USER- DATA section in the picture header. This location does not disturb the bit stream integrity and the resulting bit-stream still conforms to the MPEG-I standard. Also, this does not also cause any delay or storage requirement at the receiver, since the encrypted data arrives at the receiver after the DES key. However, this introduces a slight transmission overhead. This overhead is 88 bits (32 bits for the USER-DATA-START-CODE and the remaining 56 bits for the DES key) every time the DE§ key is transmitted. This overhead is tolerable if the key is not changed too frequently. One extreme case is to change the key for every frame. In this case, the overhead is 88 bits per frame, which is about (0.16%) of the 50,000-bit average size of an MPEG-I frame. Another extreme case is to use one key for the whole MPEG-I video sequence. The overhead in this case is only 88 bits for the entire video bit-stream. A good compromise is to change the DES key for every Group-of-Pictures (GOP). In this case, the overhead is only 0.01%. The DES key is encrypted before it is embedded in the bit stream. A public-key crypto-system such as the RSA standard algorithm is used for this purpose. This means that two keys (one is public and the other is private) are used in the encryption decryption process. This has the advantage that the crypt- analyst can not apply the same method to attack the two keys. Private Key (symmetric) and public-key (asymmetric) algorithms are normally attacked differently. This enhances the security level considerably [4]. In our implementation, the transmitter uses the RSA public-key of the intended recipient to encrypt the DES key, and the intended recipient uses his private RSA key to decrypt the DES key. Finally, he uses the DES key to decrypt the rest of the bit-stream. The RSA standard is not used directly to encrypt/decrypt the data in the MPEG-I bit stream, because it requires a long processing time [4]. This processing time is directly proportional to the size of the data to be encrypted. In this paper, we propose a 56-bit DES key; hence, the required processing time to encrypt this key using the RSA algorithm is negligible when compared to that required for encrypting an average MPEG-I frame of size 40,000 bits.

IV. Results

The overall procedure shows the following results in which first we write something on text- bar and then use image as cover medium after that these process going to be hide and encrypted simultaneously, figure (a) and b shows the original result with text data and figure c shows the saved data with stego image in some folder. For more security again we encrypt the following image with secure algorithm by which overall data are unreadable

and unopenable through which all the data are more secured figure d and e shows the overall encrypted data with stego image.


Figure a: Original image (cover) **Figure b:** Hidden text


Figure c: Stego-image **Figure d**: Encrypted image

Figure e: Encrypted image with stego image

V. Conclusions

In this paper we have presented a novel method for integrating in a uniform model cryptography and steganography. The proposed approach has many applications in hiding and coding messages within standard Medias, such as images. The algorithm has a large enough key space to resist all kinds of brute force attack. The proposed technique can be developed to generate a secret key with a different key size with different image blocks to expand its usages and with holds different attack methods. In addition, the algorithm can be developed to be used with different types of image formats to encrypt or decrypt images. Image-Stegano tool can be used by individuals or organization. This tool is platform independent and is handy for analyzing common steganography methods. Though there are several others steganography tools available but Image- Stegano can be said as combination of many tools and since it is open source so new functionalities will be added over time by volunteer contributors.

VI. Acknowledgement

I would like to extend my sincere & heartfelt obligation towards all personages who have helped me in this endeavour for their active guidance, help, cooperation & encouragement. I am extremely thankful and pay my gratitude to my project guide Mr. Abhinandan Tripathi for her valuable guidance and support on completion of this project work that always has enough time to solve everyone's problems. I also acknowledge with deep sense of reverence, my gratitude towards my parents and member of my family who has always supported me

normally as well as economically.

References

[1] .N. Al-Otaibi, & A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, Engineering and Technology Publishing, Vol. 2, No. 2, pp. 151-157, June 2014.

[2] .N. Al-Otaibi, & A. Gutub, "Flexible StegoSystem for Hiding Text in Images of Personal Computers Based on User Security Priority", Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014), December 2014, pp. 250-256.

[3] .Zhang Haitao, YEW Suet, Chen Hongyu, Zhang Ye bit planes and HVS information hiding algorithm [J]. Chinese Journal of Image and Graphics, 2013,12: 1559-1566.

[4]. Yueyun Shang, "A New Invertible Data Hiding in Compressed Videos or Images", Third International Conference on Natural Computation (ICNC 2007), Vol. 4, pp. 576-580, Haikou, Aug. 2007.

[5] .K. U. Singh, "Video-Steganography: Text Hiding in Video by LSB Substitution", International Journal of Engineering Research and Applications, Vol. 4, No. 5, pp. 105-108, May 2014.

[6]. Westfeld, A. (2001). F5-a steganographic algorithm: High capacity despite better steganalysis. In Proc. 4th Int'l Workshop Information Hiding, pages 289–302.

[7]. N. Al-Otaibi, & A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, Engineering and Technology Publishing, Vol. 2, No. 2, pp. 151-157, June 2014.

[8]. N. Al-Otaibi, & A. Gutub, "Flexible StegoSystem for Hiding Text in Images of Personal Computers Based on User Security Priority", Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014), December 2014, pp. 250-256.

[9]. A. Gutub, & H. Tahhan, "Improving Cryptographic Architectures by Adopting Efficient Adders in their Modular Multiplication Hardware", The 9th Annual Gulf Internet Symposium, Khobar, Saudi Arabia, October 13-15, 2003.

[10] .Fridrich, J., Goljan, M., and Hogea, D. (2002). Steganalysis of jpeg images: Breaking the f5 algorithm. In Proc.of In 5th International Workshop on Information Hiding.

[11] .Daniela Stanescu, Mircea Stratulat, Voicu Groza, Joana Ghergulescu and Daniel Borca, "Steganography in YUV color space", IEEE International Workshop on Robotic and Sensors Environments (ROSE 2007), Ottawa- Canada, pp.1-4, October 2007.

[12] .Cryptography and Steganography – A Survey, A. Joseph Raphael, Dr. V. Sundaram, A.Joseph Raphael,Dr.V Sundaram, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630

[13] .A Crypto-Steganography: A Survey, Md. Khalid Imam Rahmani, Kamiya Arora, Naina Pal, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014

[14] .Volume 4, Issue 1, January 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com

[15] .Volume-2, Issue-5, May-2015 ISSN: 2349- 7637 (Online) RESEARCH HUB – International

Multidisciplinary Research Journal (RHIMRJ) Research Paper Available online at: www.rhimrj.com 2015, RHIMRJ, All Rights Reserved Page 1 of 5 ISSN: 2349- 7637 (Online)

[16] .A Survey Paper on Steganography and Cryptography Z. V. Patel1st Student, M.Tech. C.U. Shah College of Engineering and Technology, Surendranagar, Gujarat (India) S. A. Gadhiya2nd Head, B.E.(IT) C. U. Shah College of Engineering and Technology, Surendranagar, Gujarat (India). 13

[17]. International Journal of Innovative Research in Computer and Communication Engineering (A High Impact Factor, Monthly, Peer Reviewed Journal) Vol. 4, Issue 1, January 2016 Copyright to IJIRCCE DOI: 10.15680/IJIRCCE.2016.

[18]. A Survey Paper on Steganography Techniques Dr. Rajkumar L Biradar1 , Ambika Umashetty2 Associate Professor, Dept. of Electronics and Telematics, G. Narayanamma Institute of Technology & Science, Hyderabad, India1 Dept. of Computer Science & Engineering, Appa Institute of Engineering & Technology, Kalaburagi, India2.

[19]. Namrata Singh, International Refereed Journal of Engineering and Science (IRJES), ISSN (Online) 2319-183X, (Print) 2319-1821 Volume 6, Issue 1 (January 2017), PP.68-71.

[20] .Namrata Singh, International Journal of Computer Applications (0975 – 8887) Volume 169 – No.7, July 2017.

[21] .Manpreet Kaur, Amandeep Kaur (October 2014) Research Article / Survey Paper : Case Study On Improved Security Mechanism Of Text In Video Using Steganographic Technique. International Journal Of Advance Research In Computer Science And Management Studies.

[22] .Hemalatha Sa. l , U. Dinesh Acharyaa , Renuka Aa Procedia B.V. Wavelet Transform Based Steganography Technique To Hide Audio Signals In Image. 47 (2015) 272 – 281 1877-0509 © 2015 Elsevier.

[23] .Vipula Madhukar Wajgade, Dr. Suresh Kumar. Enhancing Data Security Using Video Steganography, International Journal Of Emerging Technology And Advanced Engineering Volume 3, Issue 4, April 2013.

[24] .Namrata Singh, 2017 9th International Conference on Information Technology and Electrical Engineering (ICITEE), Phuket, Thailand.

[25] .Namrata Singh, International Journal of Innovative Research in Science, Engineering andTechnology,ISSN(Online):2319- 8753ISSN(Print):2347-6710, OI:10.15680/IJIRSET.2017.0602120

[26]. Intelligent Systems and Computing 810, https://doi.org/10.1007/978- 981-13-1513- 8_84.

[27] .Namrata Singh, International Journal of Computer Applications (0975 – 8887) Volume 182 – No.3, July 2018.

[28] .Namrata Singh, Journal of Image and Signal Processing Volume 2 Issue 3.

[29] .Namrata Singh, Recent Trends in Computer Science and Software Technology Volume 2 Issue