IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 4 ISSUE : 05 Print / Issue Publication Date: 09-Nov-2019

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2019.v04i05.072

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 5, ISSN No. 2455-2143, Pages 498-503
Published Online September 2019 in IJEAST (http://www.ijeast.com)

PIXEL LEVEL REVERSIBLE DATA HIDING USING TWO LEVEL ENCRYPTIONS REVIEW

Dr. Reeja S R
Associate Professor,
CSE Dept, DSU-SoE

Mr. Rino Cherian
CSE Dept., KVGCE

Dr. Jothimani K
Professor, CSE
CSE Dept., KVGCE

***ABSTRACT* - At some level of transmission of data is not secure and safe so to make the data more secure there are many methods to follow, Cryptography and Steganography are the one among them. These uses the data as an information and make them into a cipher form or just hide the existence of the data in other forms of the data then the data can be transferred in a protected way. The combinational use of both Cryptography and Steganography helps in providing the better security than the individual work of their own. The Cryptographic algorithms are used to provide two-level encryptions by converting the Original Text data into a cipher form of an integer valves with a Private Secret key whereas the Steganography converts the cipher integer values into RGB values and then modify a single pixel in each frames of the video which is selected by the user using the encryption. At the receiver's end the RGB values are obtained by the selected pixels then the integer value is obtained by these RGB values then the integer values obtained is decrypted in the first frame to the secret key, then other frames are retrieved and the integers obtained here are decrypted with the help of secret key, then the decrypted values are the ASCII values which are converted into its characters and then appended to the original message and then the message is displayed.**

Keywords: **cryptography, Steganography, Secret Keys**

I. INTRODUCTION

1.1 About the problem

Nowadays the networks are growing seamlessly and the transmission of the data is increased by its size with more than 200 percent increase. These data transmissions are used mainly for the communications between the individuals or the organizations in today's scenario. During transmission there might be an unauthorized access of the data in between or at the end of the transmission. So people wants to conserve their data which is secured, protected and transmitted safe throughout the network. The risk of losing the data is increased day-by-day by the increase of size of data. The cyber security is the main and important factor which is to be considered in the Information technology and communication fields. Every day in our daily life we often tend to use many unsecured or vulnerable networks for the data transmission.

At some level of transmission of data is not secure and safe so to make the data more secure there are many methods to follow, Cryptography and Steganography are the one among them. These uses the data as an information and make them into a cipher form or just hide the existence of the data in other forms of the data then the data can be transferred in a protected way. The technique of the Cryptography is that the data which is to be transmitted is modified into cipher form and then transmitted into the network. In the recent years there are many algorithms which are developed for the secure data transmission which uses the technique of Cryptography.

The Cryptography technique converts the data into cipher form which is always clear that the cipher is an encrypted data to the middle person. If the data is encrypted with private key, then the receiver can only be able decrypt the cipher-data by using the key. The middle person can also decode the cipher-data with different keys then result will not be same the original one. Sometimes the middle person can decode the cipher-data by using different Brute force techniques, so we people tend an another technique with Cryptography is known as Steganography.

There are to different approaches in hiding the information they are Steganography and Watermarking Techniques. Watermarking is used verify the ownership of the data when it is misused. whereas the Steganography is an art of hiding the data in data for the invisible transmission of the secret data, that is the text data can be embedded into the image with or without modifying the

original image data. This makes no suspicion on the secret data which is hidden. The security of the data can be improved by the combinational use of both Cryptography and Steganography, that is the Cryptography converts the data into another form and then makes use of steganography to hide the encrypted data in another data so that end person can retrieve the hidden cipher-data and then decrypt the cipher-data using the secret key to get the original data this process is called as Reversible Data Hiding(RDH).

1.2 **Motivation of the problem**:

Secure data transmission over a network is one of the major problems in the field of digital communication. Any type of secured mechanism can be used for safe data transfer over a network. Encryption of data to cypher text can be identified and several techniques can be used to decrypt the cypher text into readable form with the private key. Encryption converts the data into cypher form which can make sense to which the data is encrypted.

When the security of the transmission of the data is considered the person who is sending they never bother about the Space complexities and Time complexities. The person is quite satisfied when algorithms deliver same security with less Time Complexity and Space Complexity

In steganography the hacker is unaware about the existence of the text hidden in the video where a single pixel in each frame is modified to hide each character with its respective ASCII value as a reference. These pixels cannot be visualized in the high resolution video with high FPS. This gives an advantage over the normal encryption. Which makes it more secure since it is invisible to the intermediate person. Fraud during transmissions can be minimized since it is hard to decode the Original message.

1.3 **Objective**

Pixel level Reversible Data Hiding(RHD) provides the Security to the Secret text data which is to be sent through an unsecured network where the Secret text data is encrypted in two levels and then hidden in the frames of the video. The two levels of encryption follow the conversion of the text into integers using their ASCII values of each characters and then the obtained integer is encrypted into another integer form using Cryptographic algorithms with a private secret key. The secret key is used to decrypt the Secret data at the receiver's end. If end user uses any different key other than the Private secret key, they will get different message as an output.

The main objective of this project is to provide the data security through the unsecured networks with less damage in original data as well as the less Signal to Noise Ratio(SNR) values. And also make sure that there is no suspicion of the data that is hidden in the frames of the video that is in this project we are modifying the only few pixel values to hide the data if we consider a video file of high Frames Per Second (FPS) then the suspicion the data which is hidden in each frames of the video will reduce, because a human eye cannot retrace all the frame and pixels in the video. The SNR value can be reduced by using the High Resolution video with high Frames Per Second(FPS).

1.4 **Problem Statement**

We all know that the Cryptographic algorithms modify the original data into another form with different types of keys that is public and private secret key, without this the decryption of the original is impossible. Whereas the Steganography utilizes the empty spaces in the another data to store the data this is called as data hiding. This helps the transmission of the secret data without any suspicion of the encryption on it.

The combinational use of both Cryptography and Steganography helps in providing the better security than the individual work of their own. So we are using these both methods in our project. The Cryptographic algorithms are used to provide two-level encryptions by converting the Original Text data into a cipher form of an integer valves with a Private Secret key whereas the Steganography converts the cipher integer values into RGB values and then modify a single pixel in each frames of the video which is selected by the user using the encryption.

In the first Step the user able to choose the video which is to be encrypted and also provide the secret message as an input in the main user interface screen window. Then the Input text is considered as a Secret message, The Secret is converted into array of characters then the array is accessed sequentially with its index to retrieve a single character at a time until it reaches the end of the Secret Message text. When the First character is taken into the consideration and converted into its ASCII value this is the first level of encryption where the character form of data is converted into the ASCII form of integers.

At the second-level of encryption, The Cipher ASCII values is again converted into a integer form with the help of Cryptographic algorithms like RSA, ECC algorithm, Quantum Cryptography, and etc. this conversion uses a secret

key to encrypt the data. This secret will be shared to the receiver's end by encrypting it and hiding in the first frame of the video. In this level there is a randomly generated integer corresponding to the ASCII of the character which can be decrypted by the Secret key.

In the next step we use stenographic approach to hide the data in the frame by converting the integer values generated in the second-level of encryption into the RGB values to modify the pixel in the frame that values. The modification pixels in number is depends on the length of the Secret message text.

At the receiver's end the RGB values are obtained by the selected pixels then the integer value is obtained by these RGB values then the integer values obtained is decrypted in the first frame to the secret key, then other frames are retrieved and the integers obtained here are decrypted with the help of secret key, then the decrypted values are the ASCII values which are converted into its characters and then appended to the original message and then the message is displayed.

II. LITERATURE SURVEY

Jiantao Zhou, et.al (2016) says in the encryption phase, the image data hiding is done with a public key modulation mechanism where the secret key is not necessary at the receiver end. In the Decryption phase, two class SVM is used which is designed to distinguish between the encrypted and non-encrypted patches of the Image which allows to decode the embedded message and the original image. Our project uses the same decryption approach of SVM by increasing the parse time. The advantage of using the SVM in the decryption end reduces the traversal of other unwanted data where the data is not embedded. The SVM prediction rate is always similar and Cryptanalyst can analyse the patterns then decode the message since here public key modulation mechanism is used.

Zhenxing Qian,et.al(2016) shows the original Image is encrypted by the content, using a stream cipher. The stream cipher has a data-hider which compresses a series of selected bits taken from the encrypted image to make room for the secret data and it uses the Slepran-wolf encoding using the low-density parity check methods. At the receiver side, the secret-bits can be extracted if the receiver has a secret key since key defines the secret-bits in the encrypted image. This extends the retrieval of both the message and the original image at the end in our project. The advantage of using the stream cipher decreases the suspicion on the data which is hidden with in some selected bits from the encrypted image. Since the random secret bits are selected in the encrypted image, extracting the selected bits at receiver's end is difficult.

Xiaochun Cao, et.al (2016) says the use of heavily compressed pixels and the correlation between the neighbouring pixels is used to increase the amount of space to hide the secret message between the pixels this representation is called as patch-level representation. The sparse coding is used to encode the message in the space obtained. During decoding time, the spaces are obtained by the pixel correlation and the message is decoded by the secret key. The correlation between the pixels is used to build the SVM for the uncompressed image in our project. The advantage is that in a compressed images the correlation between the pixels is more which increases space to hide the data which increases the embedding rate. The only disadvantage is that image quality is reduced when compressed.

Xinpeng Zhang, et.al (2016) says during the Encryption in lossless scheme, the cipher text pixels are replaced with the new values to embed the additional data into several Least-Significant Bit planes of the cipher text pixels by multilayer wet-paper encoding. The pre-processing is carried out by shrinking the Image histogram before the encryption of image. At the receiver side the embedded data can be directly extracted from the encrypted domain and the original Image can be obtained without any loss. The data-embedding algorithms used in the encryption phase does not affect the retrieval of the Original image in the decryption phase. The advantage of using is method is to reduce the noise rate at the decryption time, that is the Original image and the message can be estimated without any loss. The reduction of the Image quality when the data is embedded in it increases the suspicion of cryptographic work.

Han-Zhou Wu, et.al (2017) proposed Reversible Data Hiding(RDH) method adopts a colour partitioning method to use the palette colours (other than the greyscale encoding or RGB encoding) to construct a certain number of embedded colour triples, whose indices are also self-embedded into the encrypted image so that data hider can be able to collect the triples to embed the secret message. At the receiver's end, the embedded colour triples can be determined by verifying a self-embedded check codes that enables the receiver to retrieve the embedded data only with the secret key. The usage of RGB encoding other than the palette colour encoding helps in the colour triples to embed the data in it. The Advantage on palette images is that they have relatively small size which can reduce the encrypted image storage space and transmission time. The payload integration is more and the

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 5, ISSN No. 2455-2143, Pages 498-503
Published Online September 2019 in IJEAST (http://www.ijeast.com)

PSNR values are high it has many applications in the real world.

Weiming Zhang, et.al (2016) says that, Similar to all Reversible Data Hiding (RDH) techniques, here the image is transferred into another image of same size. The transformed image which looks like the target image is used as encrypted image and it is easy to embed the data (secret message) into the image by any RDH methods available. Here the encryption and decryption is carried out by any of the available Reversible Data Hiding techniques. The transformation of image into another image of same size doesn't create any suspicion of the Encryption work on the image. The Original image is transformed into another image of same size and then encrypted so at the receivers end the Original image and the data can be retrieved from the encrypted image.

Fangjun Huang, et.al (2016) shows the encryption domain, RDH algorithms cannot be used because after encryption the co-relation among the pixels will change so here the pixels in a plain image are first divided into sub blocks of size m*n, then with a single key the pixels in the same block is encrypted. The correlation between pixels in each block can be preserved. We can use any RDH algorithms. Here the encryption and decryption is carried out by any of the available Reversible Data Hiding techniques. The single block has separate key for the decryption of the message with helps in better encryption and faster decoding. The advantage this framework is the it is suitable

Yun-Te Lin, et.al (2017) says that, a new data hiding algorithm for HDR images uses 3 10-bit mantissa fields as an embedding unit, it can conceal k bits of a data (secret message) using an optimal base, which gives the least pixel co-relation to hide the data. This algorithm can resist steganography analytic attacks from the HDR and LDR RS and SPAM steganalyzers. This paper presents the first data hiding algorithm for OpenEXR HDR images offering a high embedding rate and producing high visual quality of the stego images. This gives the future work on HDR images.

In this paper, Zhenxing Qian, et.al (2017) shows the algorithm enciphers an image into number of smaller parts and keeps it as a JPEG encoding format, after a content owner uploads the encrypted bit streams to a server, a data hider embeds an additional message into it, it doesn't change the bit stream size. In the receiver's end, the iterative recovery algorithm based on blocking artefacts is used to decode the message using the secret key. Since the conversion of image into smaller sizes in JPEG encoding format, the intruder doesn't have any suspicion on the data. The taxonomy diagram is shown in Fig 1.

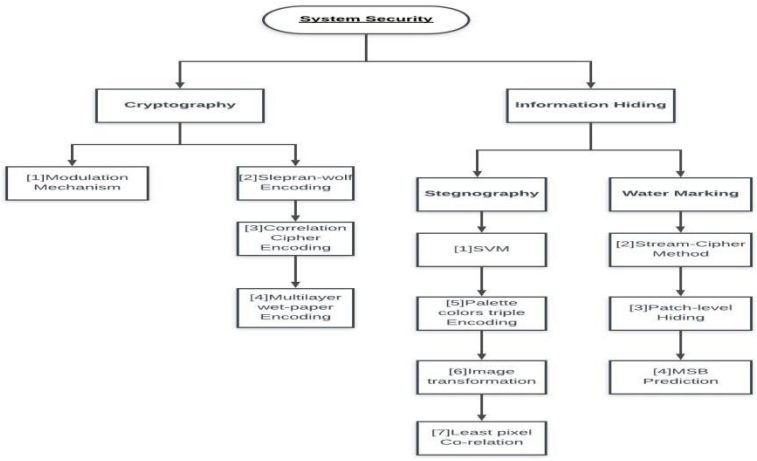

Fig (1). Taxonomy Diagram

In the proposed method, Shijun Xiang and Xinrong Luo, et.al (2018) says the groups of adjacent pixels are randomly selected, and reversibly embedded into the rest of the image to make room for data embedding. In each group, there are a reference pixel and a few host pixels in such a way that the modification on MCGs for data embedding will not cause any pixel oversaturation in plaintext domain and the embedded data can be directly extracted from the encrypted domain. On

the receiver side, the hidden cipher text data can be retrieved by employing a modular multiplicative inverse operation between the marked host ciphertext pixels and their corresponding reference cipher text pixels, respectively. After that, the hidden data are extracted promptly by looking for a one-to-one mapping table from ciphertext to plaintext. Usage of the multiplicative inverse operations to encode and decode the ciphertext pixels in the image.

Pauline Puteaux et.al (2018) shows a new reversible data hiding which is based on MSB (most significant bit) prediction with a very high capacity. There are many different approaches like high capacity reversible data hiding approach with correction of prediction errors and high capacity reversible data hiding approach with embedded prediction errors. With this method, regardless of the approach used, our results are better than those obtained with current state of the art methods, both in terms of reconstructed image quality and embedding capacity. [12] -[21] shows the background work to complete the review.

III. RESULTS

In this section, we experimentally evaluate the embedding performance of our proposed encrypted-domain. The test set is composed of 100 images of size 512 × 512 with various characteristics, including natural images, synthetic images, and highly textured images.

Fig.2 Test image

Finally, we evaluate the time complexity of performing the joint decryption and data extraction, with respect to different settings of n, where n is the number of bits embedded into one single block.

IV. CONCLUSION

By referring the above figure Fig (1), in this paper, we surveyed different cryptographic and steganographic methods which are available. In comparison with all these methods, ECC is a better method. In this paper, we design a secure system scheme which operates on both cryptography and steganography. There are two most advanced algorithms, Quantum Cryptography(QC) and Elliptic Curve Cryptography (ECC), which makes unauthorised decryption more hard to decode, making it more secure. We are using Elliptical curve cryptography method, in which an element is produced by the algorithm, which is then used to alter the RGB values of selected pixels present in every frame of the video. These RGB values produce a colour which is hidden in the pixel of the frame by replacing the original pixel.

At the decoder side, the element produced by the algorithm is subtracted from the RGB values of the data to be decrypted. The RGB value is again converted back into ASCII values of the respective alphabets. The original texts are retrieved through this process.

V. REFERENCES

[1]Jiantao Zhou, et.al "Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation" IEEE transactions on circuits and systems for video technology, vol. 26, no. 3, march 2016 441.

[2] Zhenxing Qian,et.al "Reversible Data Hiding in Encrypted Images with distributed Source Encoding" IEEE transactions on circuits and systems for video technology, vol. 26, no. 4, april 2016.

[3] Xiaochun Cao, et.al "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation" IEEE transactions on cybernetics, vol. 46, no. 5, may 2016.

[4]Xinpeng Zhang, et.al "Lossless and Reversible Data Hiding in Encrypted Images with Public-Key Cryptography" IEEE transactions on circuits and systems for video technology, vol. 26, no. 9, september 2016.

[5]Han-Zhou Wu, et.al "Separable Reversible Data Hiding for Encrypted Palette Images with Colour partitioning and Flipping Verification",IEEE transactions on circuits and systems for video technology, vol. 27, no. 8, august 2017.

[6]Weiming Zhang, et.al "Reversible Data Hiding in Encrypted Images by Reversible Image Transformation",IEEE transactions on multimedia, vol. 18, no. 8, august 2016 1469.

[7]Fangjun Huang, et.al "New Framework for Reversible Data Hiding in Encrypted Domain", IEEE transactions on information forensics and security, vol. 11, no. 12, december 2016 2777.

[8]Yun-Te Lin, et.al "A Novel Data Hiding Algorithm for High Dynamic Range(HDR)

Images", IEEE transactions on multimedia, vol. 19, no. 1, january 2017.

[9]Zhenxing Qian, et.al "Separable Reversible Data Hiding in Encrypted JPEG Bit streams", ieee transactions on dependable and secure computing, vol. 15, no. 6, november/december 2018.

[10]Shijun Xiang and Xinrong Luo "Reversible Data Hiding in Homomorphic Encrypted Domain by Mirroring Ciphertext Group", IEEE transactions on circuits and systems for video technology, vol. 28, no. 11, november 2018 3099.

[11]Pauline Puteaux "An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images", IEEE transactions on information forensics and security, vol. 13, no. 7, july 2018.

[12] Reeja, S. R., and N. P. Kavya. (2012), "Real time video denoising." , IEEE International Conference on Engineering Education: Innovative Practices and Future Trends (AICERA). IEEE, 2012.

[13] Reeja, S. R., and Dr NP Kavya. (2012) "Motion Detection for Video Denoising–The State of Art and the Challenges." International Journal of Computer Engineering & Technology (IJCET) 3.2 (2012): 518-525.

[14] Reeja, S. R., and N. P. Kavya. (2012), "Noise Reduction in Video Sequences-The State of Art and the Technique for Motion Detection." International Journal of Computer Applications 58.8 (2012).

[15] Reeja, S. R., and N. P. Kavya.(2012) "Noise Reduction in Video Sequences-The State of Art and the Technique for Motion Detection." International Journal of Computer Applications 58.8 (2012).

[16] Dias, Norman & Reeja. (2018). A quantitative report on the present strategies of Graphical authentication. International Journal of Computer Sciences and Engineering. 06. 64-73. 10.26438/ijcse/v6si10.6473.

[17] Reeja S R, Kumar Abhishek Gaurav, Ladly Patel, Rino Cherian, (2018)"*Garbage Management Using Internet of Things*", International Journal of Computer Sciences and Engineering, Vol.06, Issue.10, pp.56-59, 2018.

[18] Reeja S R, Venkat Durga Sriram, Tarun Reddy R, Venkatamanu, Rino Cherian,(2018) "*Ultrasonic Distance Measurement*", International Journal of Computer Sciences and Engineering, Vol.06, Special Issue.10, pp.42-44, 2018.

[19] Kaveri Hiremath, Dr. Reeja S. R, 2017, A Survey on Self Adjusting Slots & Dynamic Job Ordering for Mapreduce Workloads using Homogeneous and Heterogeneous Hadoop Cluster, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ICPCN – 2017 (Volume 5 – Issue 19)

[20] Kavya, Reeja S. R, Dr NP. (2014), "An Approach for Noise Removal from a Sequence of Video." International Journal of Scientific & Engineering Research, Volume 5, Issue 4, April-2014, pg.1266-1270, ISSN 2229-5518

[21] Reeja, S. R. (2014) "An Automated System for Detecting Congestion in Huge Gatherings.", International Journal of Computer Applications (0975 – 8887) International Conference on Information and Communication Technologies (ICICT-2014)

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143