A Model for Encryption of Images into Audio file - Pseudo Steganography

Apoorv Goyal, Suma Sree Thota, Sumaiya Thaseen

Abstract*: This paper aims to put forth a novel approach for the secure encryption of images. The technique makes use of superimposition of images along with signal processing techniques to achieve the proposed goal. Two keys are used for this purpose, one is a QR code generated using the mobile number of the sender and the other is a signal generated using a private value. Both the keys are used at different stages of encrypting the image. This encryption scheme follows a pixel wise encryption rather than bitwise or byte wise encryption. This way of encrypting images can be used in chat applications where end-to-end encryption is a necessity. The results obtained are convincing and show that this technique can provide robustness and security for the transfer of images. Further, the results obtained using images of different sizes as well as different keys are compared and plotted.

Index Terms*: convolution, image encryption, signal processing, superimposition.

I. INTRODUCTION

Cryptography is a very important science, used to make websites secure, and safe electronic transactions possible. Cryptography provides the following most vital services of information security [9]:

- Confidentiality: Technique used to guard information from unauthorized access or revelation.
- Authentication: Ensuring to protect information against sender forgery or spoofing.
- Integrity: Assuring users that the data was not tampered with, in between the sender and the receiver.
- Non-repudiation: To prevent the sender from denying passing the message.

Cryptography provides a strong set of techniques to ensure that the above-mentioned facilities are provided. Many cryptography algorithms already exist and many more are being formulated every day. Although there are a surplus number of algorithms, every algorithm has its own limitations and hence, there is a constant need to improve them and further develop better, more efficient ones. All these services provided by cryptography form the most integral part of any cryptographic system.

Revised Manuscript Received on 30 May 2019.
* Correspondence Author

Apoorv Goyal*, School of Electronics Engineering, Vellore Institute of Technology, Vellore, India.
Suma Sree Thota, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India.
Sumaiya Thaseen I, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India.

Any new algorithm that is designed aims to achieve one or more of these goals more efficiently than the already existing algorithms. In this paper, we attempt to propose a new technique for the encryption of images using superimposition and signal processing techniques.

The problem with existing encryption algorithms is that they provide bitwise or byte wise encryption hence increasing number of operations. In case of image, encrypting the data pixel wise provides a good enough encryption scheme and saves a lot of time and number of operations. Superimposition of images involves placing two images, preferably of the same dimension, one on top of the other. This technique is used in graphics to produce image effects, in cartography to produce photomaps, and in various other applications [10]. Usually, the images after superimposition become incomprehensible and hence this technique is very useful for image hiding purposes. Signal processing is a discipline in electrical engineering which involves mathematics that deals with the processing and analysis of analog and digital signals, and with storing, filtering and other operations on these signals [11]. Convolution is a very important technique in the signal processing domain. It is a way of mathematically combining two signals and merging them into a third signal. In the technique described, the 2D image, after superimposition, is converted into a 1D signal. This image signal is convolved with a predefined signal. A histogram of any image defines its nature. It is a graphical representation of the colors or tones in an image. A histogram can effectively act as a hash of an image as it describes the image and at the same time, it is impossible to reconstruct any image only with the help of its histogram. Rest of the paper is organized as follows: Section 2 is a concise review about the research papers referenced for this project; Section 3 describes in detail, the methodology employed in the working of the technique; Section 4 outlines the results; Section 5 describes the conclusions drawn; and Section 6 enumerates the references.

II. LITERATURE REVIEW

In [1], the security of symmetric cryptography was studied, and the pseudo-randomness characteristics of cryptographic sequences were analyzed. New methods for constructing sequences with high linear complexity were derived from this analysis. Important relations between nonlinear complexity and other cryptographic criteria were also established. Subsequently, a new recursive algorithm for computing the minimal feedback shift register which generates a given sequence was formulated which showed increased efficiency.
The paper, [2], discusses the feasibility and importance of applying a joint cryptographic and signal processing approach to multimedia encryption.

This technique was used to address the access control issues which are unique to multimedia applications. Two atomic encryption operations were proposed that are friendly to delegate processing and can also preserve standard compliance. A new system was suggested, which was theorized to provide better performance over generic encryption and its adaptation to video considering factors like bitrate overhead, security and friendliness to delegate processing. In [3], the concept of the mixed Fourier transformation is discussed, where signals are transformed to the time-frequency domain. This is mainly advantageous because here, the difference between the time and frequency disappears. Both cases of discrete and continuous time signals were considered, and the properties of mixed Fourier transformations were described. The preliminary experimental examples showed that the described mixed and root transformations can be used for signal and image processing, especially for image encryption. In [4], convolution encryption and matrical (matrix based) encryption are used to obtain a rotational and translational invariant matrix, which is free from noise, from the noisy digital image of fingerprints. A digital image of the thumbprint of a person is taken using standard fingerprint acquisition hardware. The core point of the fingerprint is detected. Fourier transform of the image is obtained and two kinds of encryption are performed on this processed fingerprint. It was seen that the image was able to be decrypted only by the authentic finger print for Matrical Encryption as well as for Convolution Encryption. Some researches [5] propose a technique based on wavelet transform for Steganography for a color image. The secret image and the cover image, which are of the same size, are deconstructed into three base color planes namely R, G and B. RGB individual planes are then deconstructed into four sub bands using Discrete Wavelet Transform (DWT). Alpha blending embedding technique is used to hide planes of the secret image within the respective planes of the cover image and then inverse DWT is applied individually. All three processed planes are combined to generate the output image. This technique was shown to provide a strong security.

III. METHODOLOGY

Fig. 1 shows how the algorithm takes an XxY image, encrypts it and converts it into a signal. The algorithm is divided into parts which are discussed as follows.

A. Generation of Key1

Key1 is generated using information that relies on common details between the sender and receiver. The information can be publicly available or hidden. In this case the use case is the chat application, i.e., Key1 is a QR code image that is generated using the mobile numbers of both the users. The mobile numbers can be directly used, or an operation can be performed to normalize the numbers into one single information block which is then converted to QR code using existing QR code generation methods.

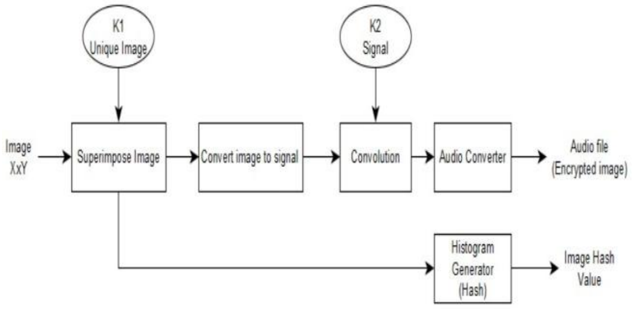

Fig. 1. Flowchart of the proposed model

The image generated in this step can also be replicated to make the key more random. The image is then resized to fit the size of the original image. Fig. 2 shows the generation of the QR code.

B. Superimposition of the key and image

The original image and the key are multiplied pixel by pixel and a new superimposed image is obtained which is a corrupted version of the original image and from which relevant information cannot be extracted. Only a person with the original key image can extract the original image from the corrupted image. Also, a histogram is generated using this image and is sent along with the final signal. This histogram acts as a hash as it satisfies all the properties of a hash. This hash value can be used to verify if the image has been modified after transmission.

C. Generation of Key2

Key2 is generated using data that is shared between the users after connection is established. It acts as a private key. Any numeric private key values that are common for both users can be used to generate Key2. Fig. 3 shows the generation of Key2. Key2 is a signal that is used for encrypting the image signal. It has some pre-decided input values that are common to the platform or the implementation of the algorithm and some user specific values which are calculated according to the users involved and act as the private key. For example, the type of signal and the number of samples can be the common feature of the algorithm used and the frequency of the signal can be calculated using the private key.

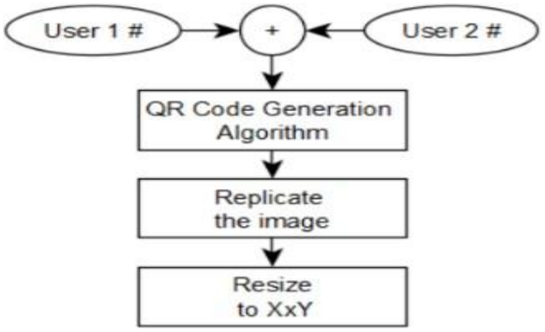

Fig. 2. Key1 Generation

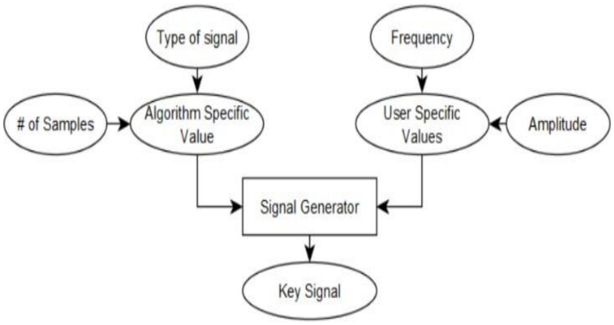

Fig. 3. Key2 Generation

D. *Encryption using convolution*

Convolution operation is one of the basic operations in signal processing and is widely used for many purposes. Discrete Convolution can be defined by the equation:

$$f[n]*g[n] = \Sigma f[m].g[n-m] \qquad (1)$$

Convolution is a reversible operation in which one signal can be obtained if the other signal is available. Convolution is used because it is sensitive to changes and small changes to the input signal can make a huge difference in the output signal. The inverse process of convolution is called deconvolution. To encrypt the signal obtained after encrypting using key1, the signal is convolved with key2 and the output is passed on to the next stage.

E. *Conversion to audio signal*

This step converts the encrypted signal obtained from previous stage into an audio signal using a sampling frequency. The conversion can be done to any of the major supported audio codec formats the only constraint being the sampling frequency should be big to extract the signal completely without losing any information. This step doesn't contribute much to the encryption but plays an important role in masking and concealing the true nature of the message. This step completes the encryption and conversion of the image to an audio file and as the image is being converted to but not hidden behind an audio file the process is called pseudo steganography.

IV. RESULTS

The outputs obtained at various stages of image encryption are shown. Fig. 4 is the QR code generated. The QR code is replicated several times for better coverage. The replicated code is then resized to enable superimposition on the image to be encrypted and Key1 is formed. The resized image is shown in Fig. 5. Fig. 6 shows the sample image which is to be encrypted. The image and Key1 are superimposed. The image after superimposition is shown in Fig. 7.

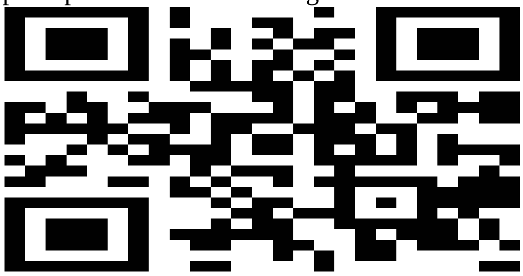

Fig. 4. QR code

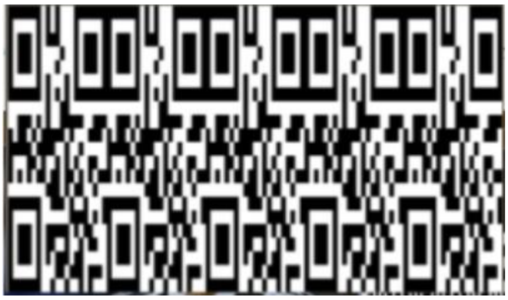

Fig. 5. Replicated and Resized QR code

The superimposed image after being converted into a signal is shown in Fig. 8. Fig. 9 represents the generated Key2. When the image signal and Key2 are convolved the results looks like Fig. 10. The histogram of the superimposed image is shown in Fig. 11. The histogram of the image after deconvolution is compared to the received histogram. If they are not equal, it suggests that the image has been modified. Therefore, the decryption process need not be completed, and the image is discarded.

Fig. 6. Image to be encrypted

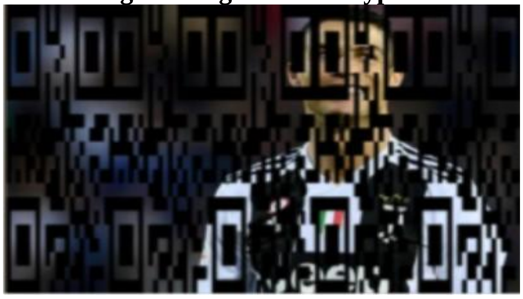

Fig. 7. Image after Superimposition

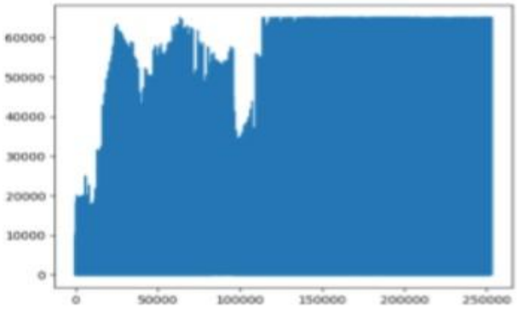

Fig. 8. Signal of the superimposed image

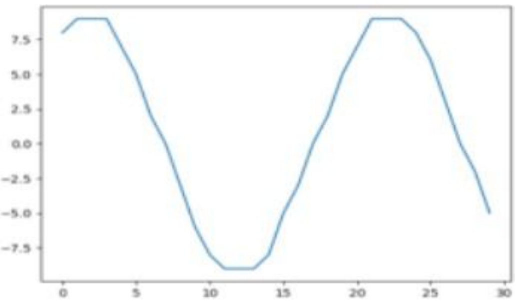

Fig. 9. Key2

The algorithm was tested for its robustness, speed and security by performing various tests. Fig. 12 shows the plot of image size vs. the encryption time taken by the algorithm. Fig. 13 shows the plot between the image size vs. the decryption time.Table1 elaborates the encryption and decryption times. Fig. 14 shows the plot between the image size vs. the size of the encrypted signal in kB.Table2 elaborates the size after encryption

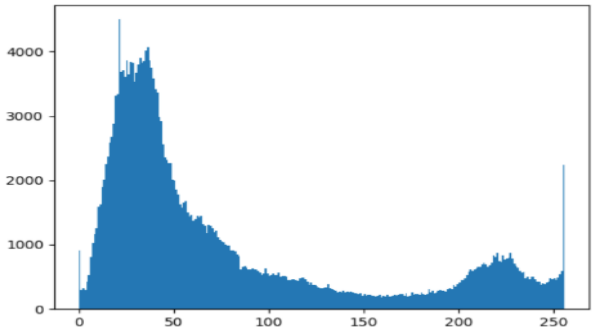

Fig. 11. Histogram of the superimposed image

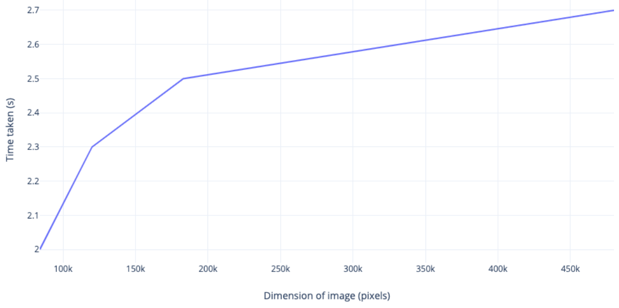

Fig. 12. Image size vs. time taken for encryption

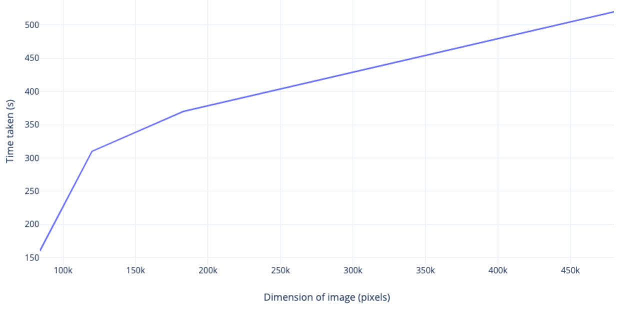

Fig. 13. Image size vs. time taken for decryption

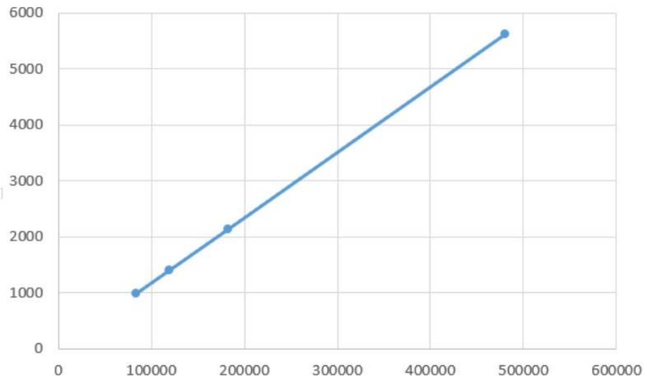

Fig. 14. Image size vs. size of encrypted signal in kB

Table 1. Various image sizes and time taken for their Encryption and Decryption

Dimensions of Image (pixels)	Time taken for Encryption (s)	Time taken for Decryption (s)
50k	2	150
120k	2.3	310
180k	2.5	370
500k	2.7	510

Table 2. Table showing the sizes of various images and the sizes of their signals after encryption.

Size of the image (MB)	Size of the encrypted signal (MB)
80	1
120	1.4
180	2.1
480	5.8

V. CONCLUSION

An attempt is made to formulate a novel approach to safely encrypt images which are being transferred in a network. The algorithm makes use of superimposition, convolution and signal processing techniques to hide an image so that it can safely be sent through a network. The histogram of the image is used as a hash to check the integrity of the image at the receiver’s side. The results obtained after executing the algorithm suggest that the algorithm is robust and secure. The algorithm also defines a linear relationship between the original image size and the encrypted signal size.

One main drawback of the approach is that, the time taken for decryption is slightly higher. Although this flaw is negligible, further research can be done to dilute this error and make the algorithm even more efficient.

REFERENCES

1. Limniotis, Konstantinos, “Signal Processing Techniques in Cryptography.” (2008).
2. Yinian Mao and Min Wu, "A joint signal processing and cryptographic approach to multimedia encryption," in IEEE Transactions on Image Processing, vol. 15, no. 7, pp. 2061-2075, July 2006.

3. N. Du, S. Devineni and A. M. Grigoryan, "Mixed fourier transforms and image encryption," 2009 IEEE International Conference on Systems, Man and Cybernetics, San Antonio, TX, 2009, pp. 547-552.
4. Ankit Misra and Gaurav Teltia, “Mixed Fourier Transforms and image encryption,” IIT Kanpur, India, April 12, 2006, unpublished.
5. Dey, Nilanjan, Anamitra Bardhan Roy and Sayantan Dey. “A Novel Approach of Color Image Hiding using RGB Color planes and DWT,” International Journal of Computer Applications, 2012.
6. Mamta Juneja, Parvinder S. Sandhu, “An Improved LSB Based Steganography Technique for RGB Color Images,” International Journal of Computer and Communication Engineering, Vol. 2, No. 4, July 2013.
7. Babita, Mrs. Ayushi, “Secure Image Steganography Algorithm using RGB Image Format and Encryption Technique,” International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 06 Jun 2013.
8. economictimes.indiatimes.com, (2019), “Definition of Cryptography,” [Online]. Available: https://economictimes.indiatimes.com/definition/cryptography.
9. wikipedia.org, (2019, April), “Superimposition,” [Online]. Available: https://en.wikipedia.org/wiki/ Superimposition.
10. tutorialspoint.com, (2019), “Digital Image Processing Introduction,” [Online]. Available: https://http://www.tutorialspoint.com/dip/image_processing_introduction.htm.

AUTHORS PROFILE

Apoorv Goyal is an undergraduate student at Vellore Institute of Technology. He is currently pursuing an Electronics and Communication Engineering degree and is involved in multiple multidisciplinary projects including but not limited to his field. He has ongoing publications mainly in the domain of artificial intelligence and signal processing.

Suma Sree Thota is a BTech student of Vellore Institute of Technology. She is currently pursuing her third year in Computer Science and Engineering with specialization in Bioinformatics. She has done many projects especially in the field of evolutionary algorithms. She has published a paper titled “Genetic Algorithm based Approach to Determine Optimal Collection Points for Big Data Gathering in Distributed Sensor Networks” in the IEEE journal. She’s been very interested in the field of cyber security and wishes to pursue a masters in that field after graduation.

Dr. Sumaiya Thaseen has thirteen years of teaching and research experience in VIT University. She completed her PhD in the domain of “Intrusion Detection Models using feature selection and ensemble of classifiers”. She has publications in the domain of intrusion detection having good citations. She has more than ten publications in the domain of intrusion detection, few of which are indexed in Elsevier and SCI. According to Google Scholar, Sumaiya has over 215 citations and the H-Index is 8. Sumaiya is a reviewer for Artificial Intelligence Review Journal.