Image Steganography based Cryptography

Jemima Dias, Dr. Ajit Danti

Abstract— The privacy and security of data is of utmost importance to individuals whose critical data can be leaked out and used for illegal purposes. The data needs to be secure and precautions needs to be taken whenever it gets transmitted from one place to another. In the preceding years, chaotic systems are erratic but definite in nature. The data encrypted using this system is so sensitive, that, changes in one of the coordinate positions leads to data being encrypted in other coordinate positions. So the proposed paper involves an image encryption algorithm, it uses a secret key from Lorenz chaotic system. It's a network consisting of weights with which the Y channel of the plain image is XORed with and the cipher image will be formed. These weights are unique and are non-identical to each other. The results have proved that the decrypted plain image has a similarity index of 0.96 to the original plain image.

Index Terms— Chaotic map, Cryptography, Image encryption, Lorenz chaotic system

1 Introduction

A technique to convert the digital form of image and implement a few calculations, and to obtain an image that is emphasized or to obtain interesting information, is called as image processing. It is a signal distribution where the input is a video frame, image or picture and output might be an image or features related to that image. So, the image processing system consists of dealing two-dimensional images while applying signal processing techniques to them. Digital Processing techniques aids in the exploitation of digital images by utilizing computers. Since the unprocessed data from imaging sensors present in satellite platform includes lots of defects, to prevent such faults and to obtain ingenuity of information, various phases of processing needs to be done. Cryptography, safeguards data and communications via code utilization so that the information aimed to receive by people expected to read and process it. In computer science, cryptography implies to shield information and transmission approaches acquired from mathematical concepts and a collection of rule-based computations called algorithms to alter messages using different approaches that are difficult to decipher. These deterministic algorithms are utilized for cryptographic key generation and digital signing and authentication to protect data privacy, web browsing on the internet and classified transmissions such as credit card transactions and email.

A cryptographic system needs to have the following properties. 1) Confidentiality: the information cannot be comprehended by anyone for whom it was unexpected. 2) Integrity: the information cannot be modified in cache or transit between sender and expected receiver without the modification being identified.

- *Jemima Dias is currently pursuing masters degree program in Computer Science and Engineering in Christ (Deemed to be) University, India. E-mail: jemimadias03@gmail.com*
- *Dr. Ajit Danti is currently a professor in Computer Science and Engineering in Christ (Deemed to be) University, India. E-mail: ajit.danti@christuniversity.in*

2) Integrity: the information cannot be modified in cache or transit between sender and expected receiver without the modification being identified. 3) Non-repudiation: the sender of the information cannot contradict at a later phase his or her intentions in the transferral of the information. 4) Authentication: the sender and receiver can verify the identity of each other and the source/destination of the information. Cryptosystems are regularly thought to imply to mathematical strategies and PC programs; be that as it may, they likewise incorporate the guideline of human conduct, for example, picking hard-to-figure passwords, logging off unused frameworks, and not talking about delicate methods with intruders. So combining both the domains, steganography is formed. Steganography, a method of concealing confidential data inside a simple message or file so that the confidential information can prevent detection; the concealment of secret data and then obtained at its destination. Steganography can be incorporated with encryption as an additional step for hiding or protecting data. Steganography is utilized to cover practically any sort of advanced information, even including text, picture, video or sound information; the confidential information can be covered up within some other kind of computerized information. The substance to be hidden is first frequently encoded and then fused into the harmless appearing spread content record or information stream. If not encoded, the hidden content is ordinarily prepared somehow or another so as to build the trouble of identifying the confidential content.

2 Related works

Owing to the hypersensitivity to prerequisites and input variables, chaotic maps have been an appealing reason for cryptographic applications for several years, creating pseudorandom and unreliable performance (Wu, Xiaolin, et al 2017). With the help of Colpitts system and the Duffing chaotic system, they can produce a 2D chaotic map where the dimensions of the map can be the same as the input image. Each pixel of the input image is traced against the chaotic map and iterated as many times as possible (Abanda, Yannick, et al 2016). Chaotic maps are executed as a combination of complex permutations and substitutions to achieve an efficient security technique.

International Journal of Scientific & Engineering Research, Volume 11, Issue 3, March-2020
ISSN 2229-5518

Using numerous Logistic maps as a foundation, the first map acts as a permuting scheme and the second map, as a substitution scheme. The prior is used to permute the arrangement of pixels and the latter is used to substitute pixel values present in the image (Yavuz, Erdem, et al 2016). The Hyper-chaotic system developed by Chen, contains phase-truncated short-time Fractional Fourier transform combined along with the encryption unit that uses permutation based on waves and puzzling substitution (Yu, Sha-Sha, et al 2020). Using 2 chaotic maps, a combination of Tent map, Sine map and Logistic map and Walsh-Hadamard transform with compressive sensing, the image is encrypted. The image uses a pseudorandom sequence to permute itself and DNA sequence operations to substitute itself (Gong, Lihua, et al 2019). Arnold cat map, a cryptic iterative permutation method with 2 secret keys is permuted and substituted for the image pixels using duffing equations with corresponding keys (Boutros, Andrew, et al 2017). The Y component of the image, is scrambled using toral automorphism found in integer wavelet transform and with the help of quantum chaotic map, the features are mixed thoroughly and a key is generated for substitution for the pixels (El-Latif, Ahmed A. Abd, et al 2013). The 2D Spatiotemporal chaotic system blends linear and non-linear chaotic map lattices and it permutes the pixels at their binary values (He, Yi et al 2018). The hyperchaotic map proposed in this paper, is derived from a complex curve which is proven by using the bifurcation diagram, attractor's correlation dimension, Lyapunov exponents . Based on the map, in the diffusion process, the plain text image pixels are jumbled and at the confusion process, the pixels are adjusted according to the XOR scheme (Boriga, Radu, et al 2014). ARX model uses 3 operations, addition, XOR, and rotation on the chaotic sequences for the confusion and diffusion process. To generate these sequences, the author uses two logistic maps (Choi, Jongseok, et al 2016). The author proposes a method which is a combination of six Bernoulli shift maps and one six dimensional Arnold map. This hybrid map utilises two-way diffusion process to generate two gray values sequences (Ye, Ruisong, et al 2013). Two maps, logistic map and Piecewise Linear map along with DNA operations consist of the encryption method mentioned in this paper. The latter map generates a chaotic image, the prior map encodes the chaotic image with the plain text image using a logistic map containing DNA rules (Wang, Xingyuan, et al 2017). The basis of image steganography, the technique of most significant bits of image pixels is introduced. Bit No. (Number) 5 is used to store the confidential content. The bit no. 5 value is changed when the difference of bit No. 6 and 5 is varied from confidential data bit. The result assures definite improvements in signal to noise ratio using the proposed method (Ammad Ul Islam, et al 2016). With the aid of an undisclosed key, the confidential information is encrypted and then inserted into the LSB of the cover image. Security is increased using visual cryptography. To make the discovery of the confidential message difficult, the altering of the pixel place of stego image is done. Using visual cryptography, the visual data is encrypted (Seema Chavan, et al 2018). Using digital encryption, the message is securely transferred. To surpass the issue of information security, affine transformation technique aids in the prevention cybercrimes (Harsh Mathur, et al 2018). In fiber optics, using light beams the data is transmitted. Light beams reduce leakage of data. For secure transmission of data, the data is first encrypted using an image and after that sent to the destination through the optic fiber in the form of light beams (Amanpreet Kaur, et al 2017). Several chaotic maps meticulously mixes optimal properties for 2D images such as using Lorenz chaotic system (Thoms, Graham, et al 2019). This paper is based on the Lorenz system since it's parameters are very sensitive that changing one of the parameters changes the position of the plot and none of the plots are identical to each other. Forming a chain network, which will contain many layers and together permute the images to form an encryption algorithm which will make the cipher images exceptionally secure and hypersensitive in nature.

3 SECTIONS

Chaotic systems are unpredictable but deterministic in behaviour. They are very hypersensitive in nature due to the initial conditions such that the exact positions are highly unpredictable. So the systems that are most suitable for encryption and decryption of images are chaotic systems since they are highly unpredictable, random and sensitive to initial conditions (Thein, Nilar, et al 2017). The Lorenz system is a set of ordinary differential equations which combine to display a point in a 3 dimensional graph using parameters α, ρ, and β. The Lorenz equation is given in (1),

$$\begin{aligned} dx/dt &= \alpha(y - x) \\ dy/dt &= x(\rho - z) - y \\ dz/dt &= xy - \beta z \end{aligned} \quad (1)$$

It is extremely sensitive to initial coordinate positions, serving unpredictable yet bounded behavior (Sprott, Julien Clinton, et al 2003).

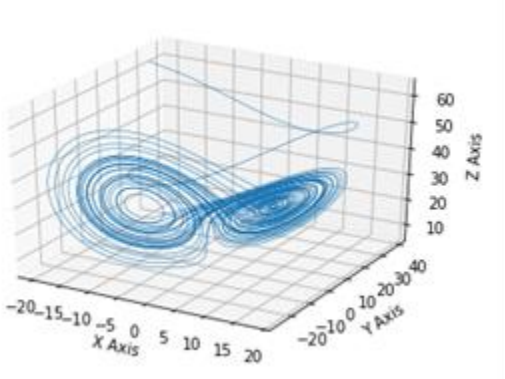

Fig. 1. The Lorenz attractor with coordinate positions as [18.69, 25.27, 65.05]

International Journal of Scientific & Engineering Research, Volume 11, Issue 3, March-2020
ISSN 2229-5518

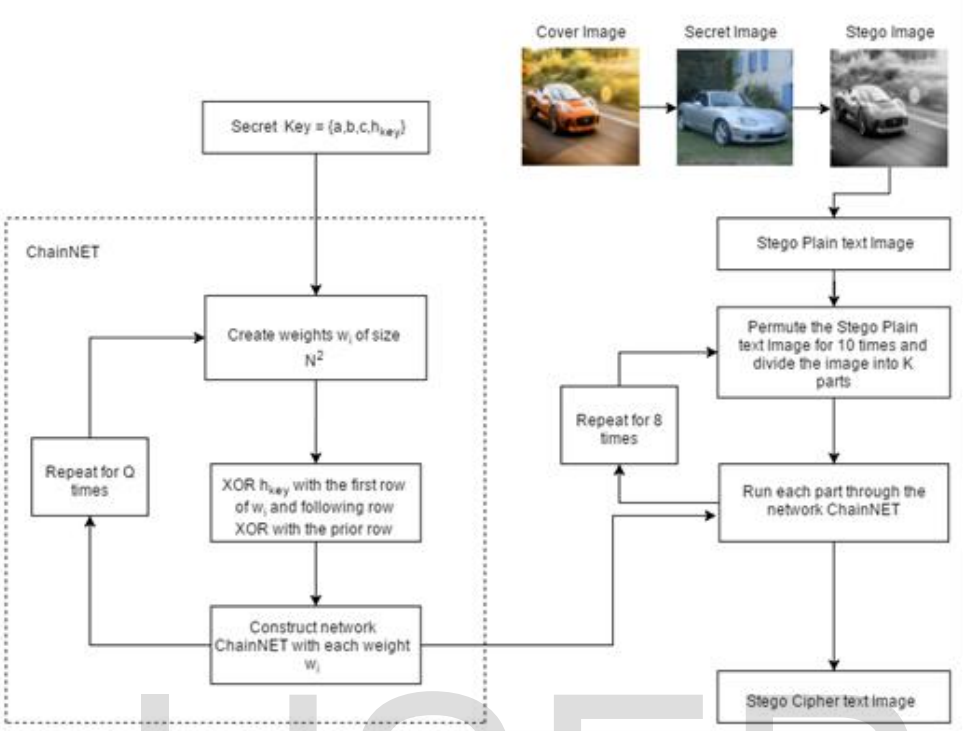

Fig. 2. Encryption Process

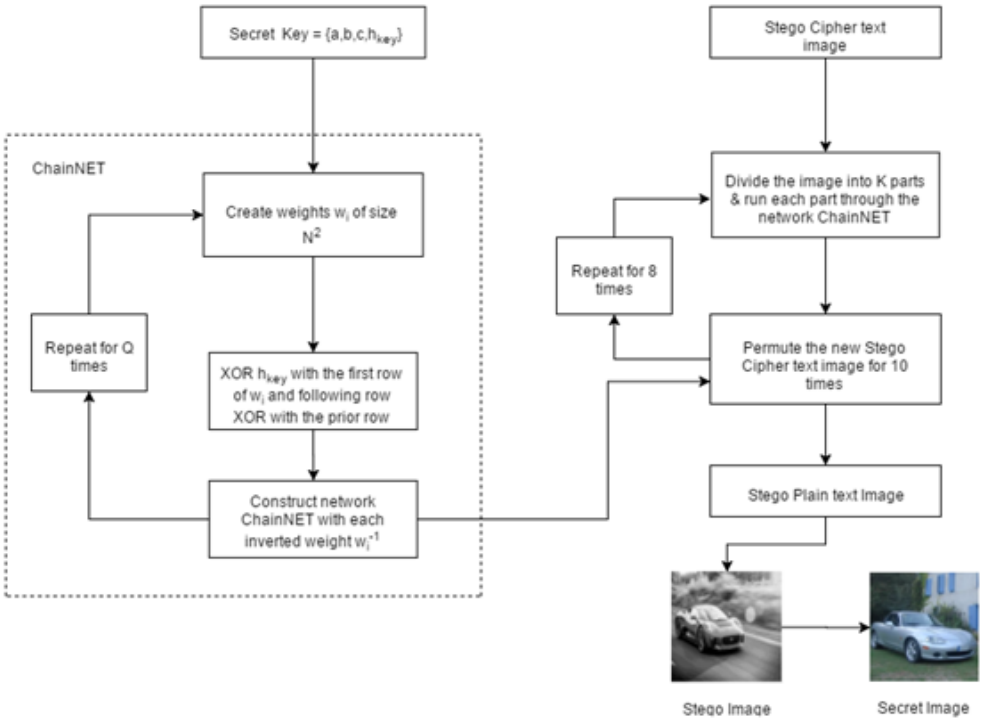

Fig.3. Decryption Process

International Journal of Scientific & Engineering Research, Volume 11, Issue 3, March-2020
ISSN 2229-5518

The method is as follows:

6.1 Encryption Algorithm

1) Select a Cover Image and a Secret image and combine both their respective grey-scale images to produce a Stego plain text image

2) Select a secret key; a, b, c, hkey. The first three parameters of the secret key belong to Lorenz system and the hkey is proportional to size of part K.

3) Create weights w of the size N2 where N is the length of the part K.

4) Then XOR the hkey with the first row of the w, and following each row XOR with each row above it.

5) Repeat steps (3-4) for as many number of weights, Q, one needs to be present in the network ChainNET

6) Apply permutation on the Stego plain text image from step (1) for 10 times and divide the newly formed image into K parts. Supply each part K to ChainNET from step (3).

7) Repeat step (6) for 8 times to get Stego cipher text image

6.1 Decryption Algorithm

1) Select the Stego Cipher text image.

2) Select a secret key; a, b, c, hkey. The first three parameters of the secret key belong to Lorenz system and the hkey is proportional to size of the part K.

3) Create weights w of the size N2 where N is the length of the part K.

4) Then XOR the hkey with the first row of the w, and following each row XOR with each row above it.

5) Repeating steps (3-4) for as many number of weights, Q, one needs to be present in the network ChainNET and produce the inverse of each weight w-1

6) Using the Stego Cipher text image, divide it into K parts and supply each part K to ChainNET from step (3). Obverse the permutation on the newly formed image for 10 times.

7) Repeat step (6) for 8 times to get the original Stego Plain text image again.

8) Extract the Secret image from the decrypted Stego Plain text image.

4 Results and Discussion

The encryption and decryption algorithm that can blend the secret data with the cover image and secret key is extremely sensitive, that a change in the parameters in itself will lead to changes of the secret image being encrypted in a different positions. A difference between the keys will provide a different encrypted images and only the specific key will be able to decrypt the output accurately. One should keep in mind that the key space needs to be large since the processing time required by the any third party attack will take some time till the actual secret key will be found.

4 Conclusion

In this paper, the image encryption and decryption method has been proposed where the secret image gets encrypted carefully into the cover image using the NET, based on using XOR operation between two images using the weights present within the network. The results have proved that the similarity index between original image and the decrypted plain image is about 0.96. For future work, one can try to use RGB images and even optimize the algorithm to get the decrypted image as similar to the original image.

References

[1] Ahmed, A.A., Li, L., Ning, W., et al.: 'A New Approach to Chaotic Image Encryption Based on Quantum Chaotic System Exploiting Color Space', Signal Process., 93, (11), pp. 2986–3000, 2013.

[2] A. Boutros, S. Hesham, B. Georgey, and M. A. A. El Ghany, "Hardware Acceleration of Novel Chaos-Based Image Encryption for IoT Applications," in Proc. 29th Int. Conf. Microelectron. (ICM), pp. 1–4, 2017.

[3] Chavan, S., & Gurav, Y. B, "Lossless Tagged Visual Cryptography Scheme Using Bit Plane Slicing for Image Processing", International Conference on Inventive Research in Computing Applications (ICIRCA), IEEE, pp. 1168-1172, 2018.

[4] E. Yavuz, R. Yazici, M. C. Kasapbaşi, and E. Yamaç, "A Chaos-based Image Encryption Algorithm with Simple Logical Functions," Comput. Electr. Eng., vol. 54, pp. 471–483, 2016.

[5] G.Thoms, R.Muresan, and A.Al-Dweik, "Design of Chaotic Block Cipher Operation Mode for Intelligent Transportation Systems," in Proc. IEEE Int. Conf. Consum. Electron. (ICCE), pp. 1–4, 2019.

[6] G.Thoms, R.Muresan and Al-Dweik, A., "Chaotic Encryption Algorithm with Key Controlled Neural Networks for Intelligent Transportation Systems," IEEE Access, 7, pp.158697-158709, 2019.

[7] He, Yi, Ying-Qian Zhang, and Xing-Yuan Wang. "A New Image Encryption Algorithm based on Two-Dimensional Spatiotemporal Chaotic System." Neural Computing and Applications, pp. 1-14, 2018.

[8] Islam, A. U., Khalid, F., Shah, M., Khan, Z., Mahmood, T., Khan, A.,. & Naeem, M. "An Improved Image Steganography Technique based on MSB using Bit Differencing," Sixth International Conference on Innovative Computing Technology (INTECH), pp. 265-269, 2016.

[9] Jongseok, C., Seonhee, S., Hwajeong, S., et al.: 'Fast ARX Model-based Image Encryption Scheme', Multimedia Tools Appl., doi: 10.1007/ s11042-016-3274-9, 2016.

[10] Kaur, A., & Soni, G, "Optical Steganography to Enhance the Speed of Analog Transmission with Security Enhancement through Image Encryption," 9th International Conference on Computational Intelligence and Communication Networks (CICN), IEEE, pp. 165-168, 2017.

[11] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An Optical Image Compression and Encryption Scheme based on Compressive Sensing and RSA Algorithm," Opt. Laser Eng. , vol. 121,pp. 169–180, 2019.

International Journal of Scientific & Engineering Research, Volume 11, Issue 3, March-2020
ISSN 2229-5518

[12] Mathur, H., & Veenadhari, S, "Blended Vector Matrix on Different Channels of Image Encryption with Multi-Level Distinct Frequency Based Chaotic Approach to Prevent Cyber Crimes by Using Affine Transformation," Second International Conference on Inventive Communication and Computational Technologies (ICICCT), IEEE, pp. 650-656, 2018.

[13] N. Thein, H. A. Nugroho, T. B. Adji, and I. W. Mustika, "Comparative Performance Study on Ordinary and Chaos Image Encryption Schemes," in Proc. Int. Conf. Adv. Comput. Appl. (ACOMP), pp. 122–126, 2017.

[14] R.Ye and Y.Ma, "A Secure and Robust Image Encryption Scheme based on Mixture of Multiple Generalized Bernoulli Shift Maps and Arnold Maps," Int. J. Comput. Netw. Inf. Secur., vol. 5, no. 7, pp. 21, 2013.

[15] Radu, B., Ana, C.D., Iustin, P.: 'A New Hyperchaotic Map and its Application in an Image Encryption Scheme', Signal Process. Image Commun., 29, (8), pp. 887–901, 2014.

[16] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical Image Encryption Algorithm based on Phase-Truncated Short-Time Fractional Fourier transform and Hyper-chaotic system,"Opt. Laser Eng., vol.124, Art. no.105816, 2019.

[17] X.Wu, B.Zhu, Y.Hu, and Y.Ran, "A Novel Color Image Encryption Scheme using Rectangular Transform-Enhanced Chaotic Tent Maps," IEEE Access, vol. 5, pp. 6429–6436, 2017.

[18] Xingyan, W., Chuanming, L.: 'A Novel and Effective Encryption Algorithm based on Chaos and DNA Encoding', Multimedia Tools Appl., doi: 10.1007/s11042-016-3311-8, 2016.

[19] Y.Abanda and A.Tiedeu, "Image Encryption by Chaos Mixing," IET Image Process, vol. 10, no. 10, pp. 742–750, 2016.