A Hybrid Algorithm for Secure Communication Using Hermitian Matrix

doi:10.3991/ijxx.vxnx.xxx (Please do not delete this line)

R.T.PaneerSelvam[1] and V.Vaithyanathan[2]

Associate Dean, School of Computing, SASTRA University, Thanjavur,Tamil Nadu, India[2]
Research Scholar, SASTRA University, Thanjavur. [1]profrtp@yahoo.com

***Abstract*—Currently secure communication is a very challenging task. Cryptography is providing solution to this challenge. But cryptography highly depends on invertible mathematical functions. Mathematical stuff embedded with computer model brings the unbreakable cryptosystem. Many algorithms are proposed in the literature and they are having their own limitations. In this paper, an algorithm based on Hermitian theory to hide a text in an image is proposed. Properties of Hermitian theory reduce the complexity of sharing a dynamic key between a sender and a receiver. The efficiency and the flexibility of the proposed model is analyzed.**

***Index Terms*—**Hermitian matrix, Encryption, Secure communication, Cryptography, Dynamic Key.

I INTRODUCTION

In the electronic world, it is mandatory to transmit information in secured way. This communication should not be affected by intruders in the communication channel. It must provide data confidentiality, integrity, authentication and authorization with data freshness. Mathematic concepts are used in encryption and decryption part. In this era, secure communication and information security play a vital role. Applications of cryptography are enormous. Today's business totally relies on e-transaction. General cryptographic algorithm is facing problem in key distribution. A traditional system uses two keys, public and private. Large transaction may not share it in prior. Again it is very difficult to identify the tool for secure communications. User may free from keeping that private key. System should be flexible enough to accommodate with any data type. Vastly available all the digital information is easy to modify, destroy and possible to duplicate. To meet this challenge, hybrid algorithm is developed. In this algorithm encrypting the original data and hide it in cover source. This stego component only sends through the channel. It also provides copyright protection techniques.

II Related Work

Cryptography and stenography is combined in this proposed work. The difference is clearly depicted in (Zaidan 2010). Traditional LSB scheme is enhanced by (Janakiraman 2012). Strength of algorithm is measured through thr capacity of cover image.(Hmood 2010) discuss over the security and capacity of the stegnographic algorithm.

Key generation, sharing and managing key is also important challenge in designing the secure communication algorithm. Power consumption and key mechanisms are analyzed by (Alioto 2010a,2010b)

Digital information may have redundant representation. This is used for hiding the image. In the redundant portion Hermitian matrix theory property is used to select the points to hide the encrypted data. For encryption also maximum eigenvalue is treated as the key. Hence two tiered security is guaranteed. This proposed algorithm need not require special key exchange between sender and receiver. It also provides extra strength to the algorithm, by reducing the key management complexity.

Several applications are brings importance to the secure communication. In which , protecting information by cryptography techniques and hiding the protected information by stegnographic techniques. For this great simultaneous job, matrix theory and hermition concepts are utilized. Finding position to hide encrypted message by hermition matrix properties is proposed here.

This paper is organized as follows. It starts with an introduction to secure system and its mathematical concepts . It brings the details of the cryptosystems and mention the limitations in the existing work. Attack types and solutions are highlighted with vulnerabilities of the system. In next section Matrix theory and its properties of Hermitian is also explained. After that proposed algorithm is explained. The experimental setup and results are listed. Finally, it proves the strength. Also, pointing the future direction in this cryptosystem with dynamic nature.The proposed system is depicted in the following two diagrams.

III Materials and Methods

To measure the performance of the proposed technique, experiments are conducted with feasible data set in MATLAB and analyzed.

Results and analysis:

1) Text to be hide is converted to ascii value and create matrix.
2) Get the cover image.
3) Reshape image matrix to square matrix.
4) Get the order of the image matrix and fix the dimension for key matrix.
5) Use symmetric concept and generate random symmetric matrix,
6) Using this symmetric , form Hermitian matrix.
7) Get the eigen values of Hermitian matrix .
8) Select the first eigen value .
9) Fix the position in the cover image based on eigen value.
10) Encrypt the ascii matrix using key matrix.
11) Convert the encrypted matrix values into binary.
12) Hide the binary in LSB position of selected bits of cover image.
13) Transmit Stego image.
14) Receiver side , get the image size and create the Hermitian
15) Get eigen value
16) Trace the positions
17) Collect LSB bit values
18) Convert Binary to ascii.
19) Use key to decrypt
20) Get the text

IV Experiment and Analysis

The proposed algorithm is tested with sample images. This implementation is done through MATLAB. Selected Pout image from Matlab image file is preprocessed. The matrix of the image is extracted and by using Hermitian matrix Eigen values are computed. Position is fixed through the size of image and encryption key is generated using the same Eigen value. The sender need not send it through the channel. It reduces the complexity of communication.

Given text is taken and processed by the key and encrypted data is embedded in the selected position of the image. The results are shown in Figure 1 and Figure2.

Figure 1 (a) is the original image and figure 1(b) is the stego image. For visualization the distortion is negligible. This can be verified with simple histogram technique. That has been shown in the Figure 2(a) and Figure2(b).

By analyzing the complexity , this reveals retrving the text is simple at the receiver side. With respect to security, this is proved with two tier strength. Hence this proposed algorithm using Eigen value from the Hermitian matrix outperforms. In future , the comparison is discussed in video stream. Information Hiding in dynamic object is tried with matrix theory.

Fig-1 (a) Original Image (b) Stego Image

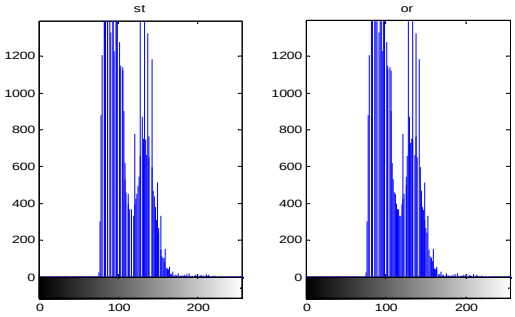

Fig-2 (a) Histogram of the Original Image (b) Histogram of the Stego Image

V Conclusion

In this paper a novel hybrid secure communication technique has been proposed. This method applies Hermitian theory to generate key for encryption and position to hide data. Since the technique utilizes the properties of Hermitian matrix ,the proposed technique is more robust against different attacks. The novelty of this paper is that the security of the algorithm is increased with the help of dynamic key and position selection to hide data. In the receiver side, extraction is possible only if properties of Hermitian is used. Robustness of the technique is justified.

References

[1] Alioto,M.M.Poli and S.Rocchi, 2010a. A general power model of differential power analysis attacks to static logic circuits. IEEE Trans. VlSI Syst.,18: 711-724.

[2] Alioto, M.,M.Poli and S.Rocchi , 2010b . Differential power analysis attacks to precharged buses: A general analysis for symmetri c-key cryptographic algorithms. IEEE Trans.Dependable Secure Comput.,7:226-239.

[3] Hmood,A.K.,H.A.Jalab, Z.M.Kasirun,B.B.Zaidan and A.A.Zaidan,2010. On the Capacity and security of stegnography approaches: An overview.J.Applied Sci.,10:1825-1833.

[4] Janakiraman, S.,R.Amirtharajan, K.Thenmozhi and J.B.B.Rayappan, 2012 Pixel forefinger for gray in color: layer stego.Inform.Technol.J.,11:9-19

[5] Zaidan, B.B.,A.A.Zaidan, A.K.AI-Frajat and H.A.Jalab,2010. On the differences between hiding information and cryptography techniques: An overview.J.Applied Science,10:1650-1655.