

Design of Robust Method for Increasing Security by Combining Cryptography, Steganography and Watermarking

¹Yogesh R. Desai, ²Sangram D. Patil

¹Dept. of E & TC, PVPIT, Budhgaon, Maharashtra

²Dept. of IT, PVPIT, Budhgaon, Maharashtra

Abstract- Now a day's security for transferring the data over a network is most important issue. There are such attacks which easily conclude hidden information or secrete data. The attempts are made to smash and picture the actual messages by the hackers and crackers. To cover up the life of message, steganography is introduced by hiding a secret message inside another trusting message. Steganography along with cryptography is used and offers more confidentiality and security over the communication channel. Steganography is a skill of hiding the important information in the other information. Cryptography is used for security purpose and Watermarking is used for copyright protection of images, audios and videos. If these three techniques are combined then system efficiency to secure the data can be amplified drastically. In this Project steganography and cryptography techniques are combined with the watermarking to increase the protection level of the particular information. The elliptic curve cryptography (ECC) technique is employed in cryptography for the security purpose and is identified as an efficient and suitable scheme for producing public key and private key. The proposed methodology has two parts. In the first part the secrete information is first converted into Elliptic curve points using Elliptic curve Cryptography (ECC) technique, this increases the robustness of the system against various attacks. In the second part watermarking technique is applied on cover image. The similarity ratio calculated shows that the watermarking is more efficient if it is embedded in the least significant bit plane rather than other bit plane. The basic idea of the proposed system is to design a simple but robust algorithm which can be easily used by average user without going into complex design.

Index Terms- ECC, Text, Image, Cryptography, Steganography, Watermarking.

I. INTRODUCTION

In today's world, security is a huge concern for our global society. Whether boarding a plane, closing the front door, or beginning your next generation circuit design, security has become a significant issue. In our homes, we try to build in the right amount of security to protect ourselves against theft. Security is rapidly becoming a necessity in the electronics industry as well. Similarly in the field of data communication also security is important, so to provide security there are many different methods of encryption that have been used.

In the last years, due to the advancement in technologies and the increase rapidly of data transmission, most people prefer to use the internet as the essential medium to transfer data. The data transmission is made very simple, fast and accurate using the internet. However, the protection and enforcement of intellectual property copyrights has become an important issue in the digital world. There are several approaches, methods and techniques have been developed to protect our information during transfer data from source to destination like Cryptography, Steganography and digital image Watermarking.

Fundamentally, watermarking can be described as a method for embedding information into another signal. In case of digital images, the embedded information can be either visible or hidden from the user. A host image used to hide the secret data is called the host image or the carrier image. After embedding the secret data into the host image, the resultant image is called the watermarked image.

In the past, people used hidden tattoos or invisible ink to convey Steganographic content. Data protection and security of the personal information have become a critical issue in the digital world. Therefore, the demand of having a protected method to transfer the confidential data is dramatically increasing. In contrast to cryptography which make data unreadable for a third party by implying some encryption methods, steganography emphasize on hiding the existence of message inside another data in such a way that nobody can detect it. According to [1], the two most common methods used for hiding information inside a picture, audio, and video files are LSB (Least Significant Bit) and Injection. In this project proposed a system, in which an image is secured by using different algorithms so as to protect the cover image data. The proposed system used various techniques during Cryptographic, Steganographic and watermarking algorithms.

II. METHODOLOGY

For the design and implementation of cryptography, steganography and watermarking the methodology followed is described below.

- To review the literature of cryptography, steganography and watermarking on and its applications.
- Deriving the suitable specifications for the implementation and also identifying the suitable algorithms for image application.
- Implementing selected algorithm using MAT Lab.
- Estimating the performance of the cryptographic, Stenographic and watermarking algorithm for future enhancement.
- To build the image application with described algorithms and measuring its performance.

Finally verifying the algorithm and system for its functionalities, quality and robustness.

The system was designed based on the requirements and functionality of the system. For the designed system, code was written and tested in MATLAB. The obtained values for different images and different data size of same image were recorded.

III. SYSTEM DESIGN

In the proposed system secrete data which is in the form of text is being secured by cryptography and steganography with watermarking so as to protect the data more easily. A combination of steganography and cryptography algorithms with watermarking technique which provides strong backbone for its security. This proposed system not only hides large volume of data within an image, but also limits the perceivable distortion that might occur in an image while processing it. This proposed method has an advantage over other information security systems because the hidden text is in the form of images, which are not obvious text information carriers.

The Proposed system has following steps:

1. Registration
2. Encrypt text information
3. Embed the text information
i.e. Steganography
4. Embed the Logo i.e. Water marking
5. Decrypt that information to another language of environment

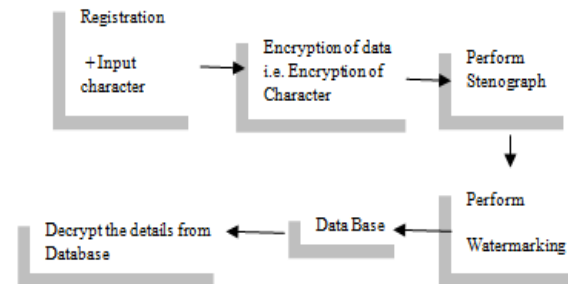


Fig.1.The Overall System Design

IV.SYSTEMIMPLEMENTATION

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Cryptography scrambles the message so it cannot be understood; the Steganography hides the message so it cannot be seen. Combining these two methods together for the purpose of developing a system that will improve the confidentiality and security of the message. Moreover here including watermarking method so that it will give the authentication and we used invisible watermark method to hide the watermarked data inside the cover image.

However, it is always a good practice to use Cryptography and Steganography together with Watermark for adding multiple layers of security. By combining, the data encryption can be done by a preferred method and then embed the cipher text in an cover image or any other media with the help of stego key and then the cipher text is authenticate by inserting watermarked image which is invisible. The combination of these three methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. The figure below depicts the combination of Cryptography, Steganography and Watermarking.

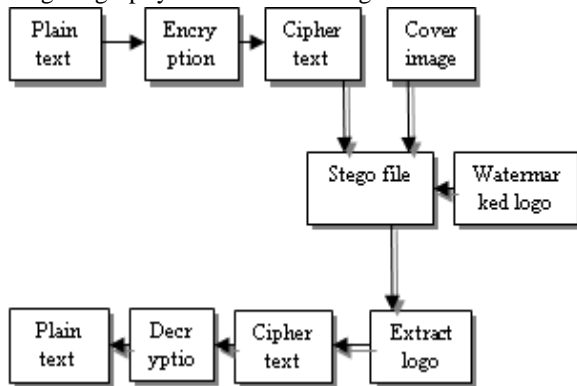


Fig.2: Combination of Cryptography, Steganography and Watermarking

The above technique is combination of Cryptography, Steganography and watermarking. In this cipher text is embedded in to stego file which is nothing but cover image as well as watermarked image since here performing watermarking on same image.

V. CONCLUSION

In this proposed system, combination of Cryptography and Steganography with Watermarking is designed which could be proven as a simple but highly secured way for protecting secrete information in the field of data communication. Steganography especially combined with cryptography and watermarking is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality with very little distortion in the image. The main advantage of

this System is to provide high security for key information exchanging. It is also useful in communications for codes self error correction. It can embed corrective audio or image data in case corruption occurs due to poor connection or transmission.

The proposed High secured system using a comparative study from the survey of previous methodologies about the cryptography, steganography and watermarking has been made. High performance architecture for point-double multiplication, the key operation of ECC, has been proposed. Due to complexity of finding kG integers here not concentrating on cryptanalysis, but the proposed system established much higher robustness and security. Also consider the effectiveness of LSB during on cover image employed to encode the message inside the image file and watermarking technology for authenticating. The system therefore makes its security more robust.

VI. FUTURE WORK

Future enhancement can be done by implementing the proposed algorithm in the hardware. Robustness can be increased by embedding entire Watermark logo into the video frames. Meanwhile complexity can be added in secret key generation to increase the security level. Speech, text, image and video itself can also be used as watermark.

REFERENCES

- [1] Sridevi R, Damodaram A, and Narasimham S. "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key With Enhanced Security" Journal of Theoretical and Applied Information Technology (JATIT), Vol.5, pp.768-771, 2005.
- [2] M.Grace Vennice, Prof.Tv.Rao, Swapna and Prof.J.Sasi kiran."Hiding the text information using Steganography." International national journal of Engineering Research and Application (IJERA),ISSN: 2248-9622 Vol. 2, pp.126-131,Jan-Feb 2012.
- [3] Sarita Poonia, Mamtesh Nokhwal, and Ajay Shankar. "A Secured Image based Steganography and Cryptography with Watermarking" International Journal of

- Engineering Science and Engineering (IJESE), Vol.1, pp.66-70, 2013.
- [4] Abikoye Oluwakemi, Adewole Kayode S and Oladipupo Ayotunde J “Efficient Data Hiding System using Cryptography and Steganography” International Journal of Applied Information Systems (IJ AIS), Vol.4, pp.6-11, 2012.
- [5] M. Bellare and P. Rogaway. “Optimal Asymmetric Encryption-How To Encrypt With RSA” International conference on advances in Cryptography-Eurocrypt techniques, Vol.950, pp.92-111, 1995.
- [6] M. Bellare And P. Rogaway. “The Exact Security Of Digital Signatures-How To Sign With RSA and Rabin” International Conference on Theory and Application of Cryptographic Techniques, Vol.96, pp.399-416, 1996.
- [7] N .Provos and P. Honeyman, “Hide and Seek: An introduction to Steganography,” IEEE transaction on Security & Privacy Journal, Vol.1, pp.32-44, 2003.
- [8] S.Lyu and H.Farid, “Steganography using higher order image statistics,” IEEE Transaction on Information Forensics and Security, Vol.1, pp.111-119, 2006.
- [9] Gustavo D. Sutter, Jean-Pierre Deschamps, and José Luis Imaña “Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations” IEEE Transactions on Industrial Electronics, Vol. 60, pp.217-225, 2013.
- [10] Reza Azarderakhsh and Koray Karabina “A New Double Point Multiplication Algorithm and its Application to Binary Elliptic Curves with Endomorphisms” IEEE Transactions on Computers society, Vol.62, pp.1-7, 2013.
- [11] Mohamed Radouane, Tarik Boujiha, Rochdi Messoussi, “A Method of LSB Substitution based on image blocks and maximum Entropy”, International Journal of Computer Science Issue, vol. 10, issue 1,no 1,January2013.