Combination of Cryptography and Steganography for Data Hiding

Rashmi Borsutkar[1], Madhuri Lokare[2], Shraddha Subhedar[3]
Information Technology[1, 2, 3],
Saraswati College of Engineering[1, 2, 3]
Email: rashmiborsutkar@gmail.com[1] ,madhuri.lokare27@gmail.com[2] ,shraddhasubhedar23@gmail.comr[3]

Abstract-.This paper discusses about data hiding, in which the pixels are randomly selected and higher nibble bits are matched with it. A two bit code will be generated to encode the matching bits. This system can be used to improve security level for information being transferred over open channel. It is a practice of encoding/ embedding the secret information in a manner such that the existence of information is invisible. Digitization of analog signals has opened up new avenues for information hiding and recent advancements in the telecommunication. Digital images are most common cover files used for steganography. It comparatively evaluates the performance of gray scale and color versions of a given steganography method.

Index Terms- 2Bit code, security in data transmission

1. INTRODUCTION

Cryptography is a means for granting secure communication between individuals, military forces and government agencies**.** Steganography is the art of communicating in such a way that the presence of message won't be detected. Bit positions in the higher nibbles of the cover image at a position indicated using a 2-bit code is used for data hiding. Organizations and Individuals around the world rely on the ability to ensure data and communication systems are secure and reliable. Information security allows users to access services, authenticate the origin and integrity of software and other data and verify the identities of other users and organizations. The image with the mysteriously embedded message given by the encoder is the *stego-image*. The stego image should be identical to the cover image under casual inspection and analysis. In addition, the encoder usually uses a *stego-key* which assures that only receivers who know the corresponding decoding key will be able to derive the message from a stego-image.

In an information exchange world, most of the data is transferred through an open channel or network such as Internet which is vulnerable to interception. This might leads modification or deletion of important data. To avoid these undesirable acts, steganography and cryptography are used together to ensure security of the data.

Steganography is derived from Greek for covered writing. Steganography is the art of writing messages in a way that no one apart from the sender and intended receiver even realize the hidden message in the image. Cryptography is also derived from Greek for secrete writing.

Cryptography consist of encryption and decryption ; Encryption means plain text original text converted into a cipher text and decryption means cipher test s converted into plain text or original text. For encryption and decryption secrete key is required. DES, AES, RSA, MD5 and Diffie Hellman algorithm is used in cryptography.

In steganography, digital medium is required for embedding. Images and multimedia components, such as audio and video files, are widely used and exchanged through the internet. The best thing about the steganography is that it hides the existence of secret communication.

Data hiding is an important theory in any networked system as there are many hackers and intruders present. So we have to use data hiding techniques so that our data is secure and no one can manipulate or even know that any some sort of data is present there. When some unauthorized person gets access to your asset then this attack is known as interception.

2. DIGITAL IMAGES

The data that the sender wishes to send to desired receiver using digital image can be done .The cover is the medium which serves to hide the presence of message which is embedded, it is also referred to as a message wrapper [1]. It is not mandatory that the cover and confidential data have homogeneous structure. Recovering the message form stego-image requires the stego-key for decoding purpose, which was used for encoding. A secret copyright or watermark can be embedded inside an image to identify as authenticated property. Timestamp, annotation and other descriptive elements can be

embedded in an image such as place, names of individual, thing, etc.
There are some of the features of steganographic approach. Hiding capacity is the capacity of the cover image to store or hide data into it. Perceptual transparency is the distortion in cover image while embedding the secret data, which should me minimum. Because even if the attacker knows that the image consists of secret information, but couldn't get that secret information, even then the technique has failed.

Robustness refers to the ability of secret info to stick to the stego image even after various alterations to the cover image. Tamper resistance is the difficulty of an attacker to alter message once it has been embedded into stego image.

3. EMBEDDING METHODS

3.1 Least significant bit encoding

It is a technique in which the bits of message are embedded directly into LSB position of cover image. The output image so obtained cannot make out the difference or manipulation done. Steganos is a LSB embedding system that can embed data inside a variety of image, audio and text covers. Stegano was able to recover the message when stego image was made available for decoding.

If the LSB of the value of pixel ***I*** (*i*, *j*) is equal to the message bit *m* to be embedded, ***I*** (*i*, *j*) remains same. If not, set the LSB of ***I*** (*i*, *j*) to *m*.

Secret messages can be embedded in LSB plane by sequential or random LSB replacement. Sequential LSB replacement can be carried out more conveniently but has a much serious security problem in that there is a likely difference (statistical) between the modified and unmodified part of the stego-image. By random LSB replacement, the secret messages can be randomly scattered in stego-images, hence improving steganographic security.

Discrete Cosine Transform (DCT), Discrete Fourier Transform, or Wavelet Transform can offer higher robustness against lossy compression as they are designed to resist or exploit lossy compression algorithms.

3.2 Transform embedding technique

It offer increase robustness w.r.t scaling, rotation or cropping. Jpeg-Jsteg is software that embeds the message by modulating DCT coefficients of stego-image based upon bits of message and round off errors during quantization. The watermark or message can be considered as a narrowband signal encoded in a larger frequency band. Two dimension Wavelet Transform is based on one dimension filtering along horizontal and vertical directions. Four sub bands LL, LH, HL, and HH are obtained from the first level 2-D Wavelet Transform by extracting edges, i.e., regions containing high-frequency, along diagonal, horizontal, vertical or orientation from the original image. However, edges usually exist in other directions. Filtering which do not fit "curves" (concatenating edges) in image increase energy in high-frequency sub bands.

3.3 Perpetual masking

Masking refers to a phenomenon in which a signal can be imperceptible to an observer in the presence of another signal. The masking property makes it difficult for anyone to find out message from that segment, for ex.-it makes one difficult to find randomly placed needle in a haystack, the needle can be in a plane view to an observer yet the observer will have difficulty locating the needle

3.4 Robust method for hiding ASCII characters

It is based on the matched between the bit value of randomly selected pixel P from cover image and data bits. This robust method improves robustness compare to least significant encoding technique. In this, select any pixel randomly and scan the higher nibble of that pixel with the data bit. Store position of the pixel as 2-bit code at bit pair positions (1,2) ,(2,3) , (1,3) , (2, 4) , or (1,4) assigning (00) , (01) , (10) and (11) for *P* = 5, 6, 7, and 8 respectively. Skip the pixel if matched is not found between the pixel bit and the data bit. For the retrieval data apply reverse process. Then extracted data bits are arranged in their original order to complete the retrieval process.

The new robust method decrease the perceptual distortion of the cover image because of the higher nibble of the pixel is not altered. This technique can be used effectively in open channel and also avoids the eavesdropper attention to attack the stego-image.

3.5 Digital steganography

It means hiding data within the data. Digital steganography is the art of modestly hiding data within data. For digital steganography, image watermarking is used for copyright protection. Digital watermarking is a method to embed the secret information or watermarks into the image which is used to protect the ownership of image. There are two types of watermarking method: visible watermarking and invisible watermarking. Visible watermarking is easily visible to human eye such as company logo, television channel logo. Whereas, in the invisible watermarking approach, only authorized person can extract the data.

4. STEGO-ANALYSIS

The practice of attacking steganographic methods by detection, destruction or modification of embedded data. By understanding the way in which attacker can defeat steganographic system is required is requires for design and development of more robust system. An attacker can be considered as a successful one according to its application .sometimes even if the detection is made of some kind of data is hidden in stego image, it is considered as a successful attack. For pirate attempting to defeat copyright mark, one should not only detect the mark but destroy or modify the mark without significant degradation of quality of that stego image.

Cryptanalysis & Steganalysis, both fields assume that the attacker is able to understand the method used to encrypt or hide data. Which means the entire secrecy of the method will be in the selection of the encryption or stego key and not in the intricate working or proprietary nature of method.

There are various categories of steganalysis :-

Stego only steganalysis - means only stegoimage is available for steganalysis. It is the weakest form of attack.

Cover attack - both the original cover and the corresponding stego image is available.

Known message steganalysis - is when the steganalyst knows the secret message in stego image.

Choose stego steganalysis - means when the access to message extraction tool is available so that the attacker doesn't have to deduce the decoding algorithm.

Chosen message steganalysis - is the most powerful attack in which steganalysis has access to steganography encoding tool itself and can embed and analyse messages of its own choice.

In new passcode based approach for hiding secret information in image explains different techniques about embedding the 2 bit code using embedding word called as password. The new passcode based technique is similar to the new robust method of hiding, but it defines how to deal when no match is found between the data bit and pixel bit.

Randomly select pixel M of the cover image and then match higher nibble of that pixel with the data bit. Generate the 2BC associated with the matching 00, 01, 10 and 11 representing positions 5, 6, 7 and 8 respectively. If no match found, assume 5th position is matching. This is a special case of a passcode based approach. Now repeat the above step for embedding all the bits. To embed a 2BC, code selects another pixel randomly. Only the lower nibble of newly selected bits is used for storing the 2BC. Then password which is known by only sender and receiver is converted into binary form. If the password bit is '0', then the first bit of 2BC is stored in position 1, else it is stored in position 2. The second bit of 2BC can be saved using different techniques.

1. (1) Directly send the second bit of 2BC to receiver. This technique slightly reduces the level of security and quantity of embedding data.

2. (2) Store the second position in a fixed location such as position 3 of the pixel.

3. (3) Save the 2nd bit in a specific order.

4. For example, the first 10 bits are hidden either in position 1 or 2, whichever is available after embedding the first bit of the 2BC, the next five bits are hidden in position 3 and next bit is hidden in position 4. After storing all the bits we get the stego image. Now this stego image is send to intended receiver.

At receiver side, same randomization algorithm is applied to select pixels named M and E, which are the pixels used for matching the data and embedding the 2BCs based on password. Depending upon the password bit first bit of 2BC is extracted, if the password bit is '0', then the first bit of 2BC is extract from position 1, else it is extract from position 2. The second bit of 2BC can be read depending on the technique used for embedding. The extracted bits are then combined to obtain the different 2 Bit Codes. The data bits are extracted from the *M* pixels based on the position obtained from the 2BC's. When the position is '5', the receiver will check if the bits in positions 8, 7, 6 and 5 are the same. If they are same, then this case corresponds to a "no match" and hence the complement of the bit in position 5 is taken as the data bit, else the same bit is taken.

This new passcode based approach maintains good perceptual quality and also imperceptibility.

CONCLUSION

We have surveyed different techniques which combines different approaches in cryptography as well as steganography to achieve security in communication to some extent. These methods can be used in staggering in growth communication technology to keep the data safe from vulnerabilities, threats and unauthorized access. As Steganographyis used in these techniques it also provides higher immunity to hidden data.

REFERENCES

[1] E. T.Lin and E. J. Delp, "A review of data hiding in digital images", CERIAS Tech. Report, no.149, 2001

[2] T. Zhang, Y. Zhang, X. Ping, and M. Song, “Detection of LSB steganography based on image smoothness”, Proc. IEEE Int. Conf. on Multimedia and Expo., Toronto, Canada, July 9-12

[3] H.V.Singh, S.P. Singh, and A. Mohan, “A new robust method of hiding text characters for secure open channel transmission,” Int. Journal of Computer Science and Network Security, vol.7, no.7, pp. 31-36, 20072006, pp.13771380.

[4] Technologies, Karur, India, July 29-31, 2010, pp. 1-6. P. Marwaha and P. Marwaha, “Visual cryptographic steganography in images”, Proc. Int. Conf. on Computing Communication and Networking

[5] D. Kahn, Information Hiding: First International Workshop, R.J. Anderson, Editor, Cambridge, UK: Springer-Verlag, 1996, vol. 1174, Lecture Notes in Computer Science, pp. 1-5.

[6] A New Passcode Based Approach for Hiding Classified Information in Images Vishwanath Ullagaddi Firas Hassan Brent D. CameronDouglas Nims Vijay Devabhaktuni.