International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 04 | July-2015 www.irjet.net p-ISSN: 2395-0072

A Comprehensive Survey on Data Hiding Technique

Pawan R Sharma[1], Jitendra Mishra[2]

[1]M Tech Scholar Dept of Electronics& Communication, PCST Bhopal, INDIA

[2]Asst Prof Dept of Electronics& Communication, PCST Bhopal, INDIA

---***---

Abstract - *In the current scenario, world is facing heavy data exchange, the security, integrity and reliability of data is crucial aspect behind this process the study conducted in this survey review different data hiding techniques such as watermarking, steganography, cryptography, mosaicing on properties which are important during the exchange process the unwanted variation in this properties may cause data leakage or may get stolen. In this manuscript we have reviewed on parameters like Hiding Capacity, Robustness, Security, and Reliability.*

Key Words: Mosaicing, secret fragment visible, Steganography, watermarking, Cryptography

1. INTRODUCTION

Today social interaction leads the data transfer and is carried by several means, virtue of fast internet facility. The data can be in the form of image, video, audio or text (personal or organizational) is confidential. As the web is not a secure place, leakage of data can leads to disasters impact on social as well as personal life. The most important aspect in transferring data is threat of hackers, leakage of information in exchange process.

Several techniques has been adopted for protection of data, the review and study of those process should be done thoroughly while adopting a single or multiple process. The security of data is most important aspect of the whole exchange process. In this review we analyzed the following properties for data hiding techniques.

- Hiding Capacity
- Robustness
- Security
- Reliability

Hiding Capacity: It is the size of data that can be hidden to the size of cover, (watermarking, mosaicing, steganography) which is used to hide the data, during exchange of data.

Robustness: It is the ability of the system to overcome an error during the process, in data hiding the embedded data has to remain intact under transformation.

Security: This is the most important property for the system; the security of the embedded information has to be very high, here the eaves-doper, data loss, no of attempts to guess the permutation is an important aspect during design of algorithm for the system.

Reliability: It's an important property which guarantees the delivery of data to the reception.

The above properties are ideal in structure and functioning of the system which comprise wired, wireless and various models. Security is foremost important in hiding and un hiding of the data, in following section we analysis different method available for securely transmission of data.

2. LITERATURE SURVEY

2.1 Watermarking

The history of watermarking is hundred of year back; it all started in handmade paper industries which used to identify the company producing paper, quality and strength. The paper watermark in bank notes and stamps inspired the first use of the term watermark in the context of digital data.

The watermarking scheme embeds watermarks into signal or transformed version of the signal, the signal has to be very robust against all attacks and damage of image. The key helps to validate the signal which is been compared and extract the watermark signal. The process is classified into two types visible watermarking and invisible watermarking. The main goal of watermarking is to hide message in one too many communications.

Application of watermarking:

1. Forensics and piracy deterrence

2. Broadcast monitoring

3. Improved auditing

4. Authentication of data

All kinds of the data can be watermarked video, 3D models, text, animated models

Figure 1 show the embedding process, input to the scheme is the watermark data the secret or public key and the method to embed

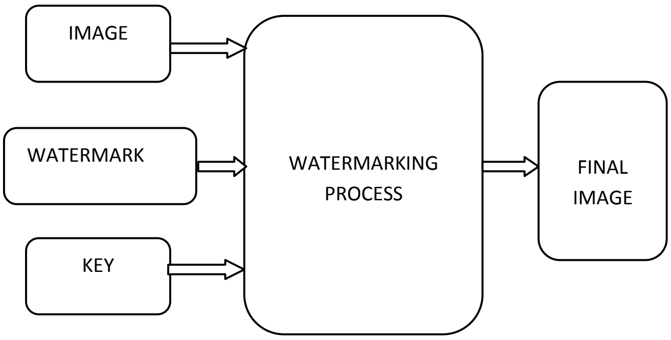

Figure 1 Block Diagram of Watermarking Embedding Process

Advantages:

1. Uniquely identifies the owner of copy right work

2. Embedding watermark is easy

The main disadvantage is it doesn't prevent image copying but can track down and detect ownership, other is image distraction

2.2 Steganography:

Stegano`s: covered, Graptos: writing which means 'cover writing'. The main goal of steganography is to hide a message M in video, audio, image or text data D, to obtain embedded new data DN, practically indistinguishable from D during exchange in such a way that hacker can`t remove or replace M in DN,

The steganography can embedded the secret message in audio video image or text just by imperceptibly adjust the bits of pitch of sound life, encoding the secret text by adding small variation or alters the pixel of the image. During transmission, the embed data with these small difference do not appear to change the file and human ear and eye can`t detect it.

The main goal of steganography is to hide a message in one-to-one communications.

Applications:

Secure secret communication

Military applications

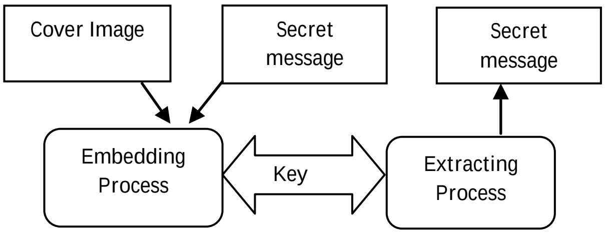

Figure.2 Transmitter and receiver process for Steganography

Advantages:

It does not attract attention

Difficult to prove it exits

Make internet surveillance difficult

2.3 Cryptography:

Cryptography is the technique for secure data exchange where electronic message is converted into cipher text. When we are using internet for mail, online shopping, funds transfer we are entering sensitive data such as name, email address, physical address, phone number, PIN and password but security is major concern on the internet there a whole of information we don`t want other to see. So security is provided by different method, one type is cryptography.

The system is based on one of the following types

1. Symmetrical key encryption

2. Public key (Asymmetrical) encryption

In symmetrical key method a private key is used to exchange the data to be shared, where as in Public key encryption technique a combination of public and private key is used for exchange of data.

Application:

In E-Commerce

Data Base Security

Data in Network security

In ATM cards

Advantages:

Very high speed of encryption

Uses password authentication to prove receiver identity

Uses digital signatures

Disadvantages:

The main disadvantage is cryptographic algorithms patents, and the other is it hides the content of the message, not the existence of the message

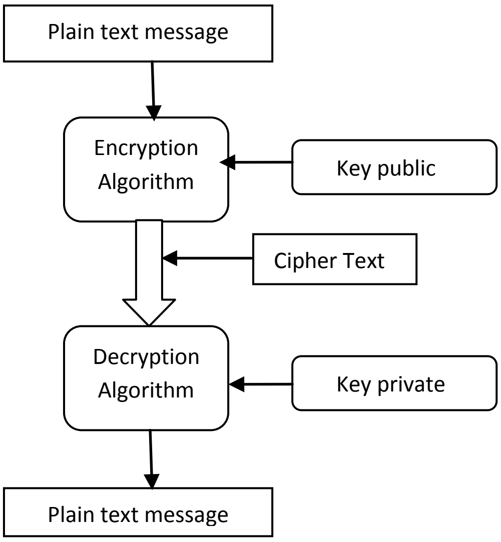

Figure.3 Encryption and Decryption process for cryptography

2.4 Image Mosaicing:

The two common approaches for image transmission are image encryption and data hiding, the encryption method uses the natural properties of the image, where as the data hiding technique utilize the histogram shifting, LSB substitution, the main issues is hiding is the large amount of data to be embedded in single image. The mosaic image is the solution to this, proposed by Lai and Tsai. Ya Lin Lee and Tsai made some improvement in.

In the proposed method a secret image is transformed into a meaningful mosaic image and controlled by key. The system is divided into following stages

1. Select target image

2. Image splitting

3. Creating mosaic image

4. Embed process

5. Retrieve secret image

The algorithm is divided into two parts mosaic image creation and the recovery of embed secret image

Algorithm 1: Mosaic Image Creation

Step1: Target image is selected, it can be random or from database

Step 2: Fitting the tile image in the target blocks

Step 3: Performing the color transformation between tile images and target blocks and rotate tile image with respect to RMSE values.

Step 4: embedding the secrete information

Input: a Secret image IS a Target image IT and a secret key K

Output: A secret mosaic image IM

Algorithm 2: Secret Information Recovery

Input: A mosaic image IM with n Tile image and Secret key K

Output: the secret image IS.

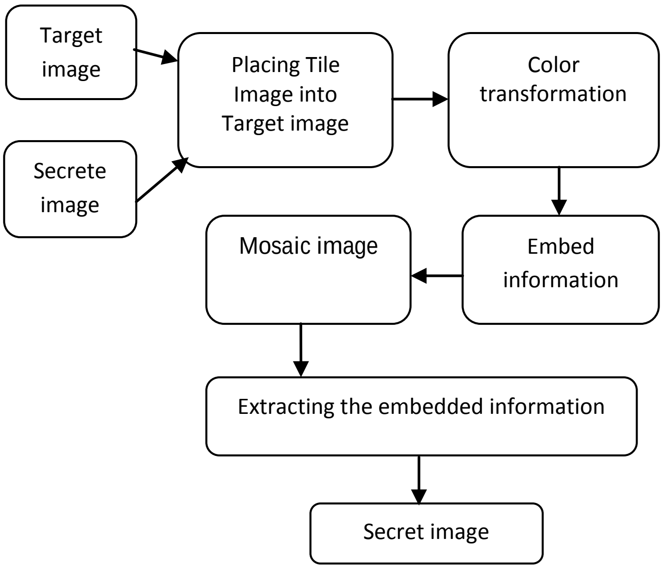

Figure.4 Block diagram of image mosaicing process

Security Consideration:

The security issues are address very well here the embedded information is encrypted with the secret key. The no of all possible permutation is P = 1/n! If guess correctly, hacker has to know the correct parameters for recovering the original color appearance of image as it is encrypted as bit stream using secret key.

Limitation:

The size of available target image should match that of secret image, if the target image is enlarged it may cause the mosaic image to blur so the care has to be taken to select the appropriate size of target image.

3. COMPARISON BETWEEN DIFFERENT DATA HIDING TECHNIQUES

Table 1 Comparison of different data hiding techniques

Parameters	WM	STG	CRYP	MOS
Hiding capacity	Medium	Medium	High	High
Robustness	Medium	Medium	Good	High
Security	Medium	Medium	High	High
Reliability	Medium	Good	Good	High

WM: Watermarking STG: steganography

CRYP: Cryptography MOS: Mosaicing

4. CONCLUSION

Data hiding techniques gained attention of researcher with its reliability, Security, Robustness and Hiding capacity, while rethinking and reviewing data hiding techniques watermarking, steganography, Cryptography, Mosaicing with the same parameters it has concluded that the Mosaicing techniques is more secure with respect to its security level, data handling capacity and reliability. While adopting any of the techniques in single or multiple processes all these parameters are to be taken in consideration for security of the data.

5. REFERENCES

[1] Ya Lin Lee, Wen-Hsian-Tsai, "A New Secure Image Transmission technique via secrete-Fragment-Visible Mosaic Image by Nearly reversible Color Transformation" IEEE transaction on circuit and system for video technology, Vol 24, No 4, April 2014

[2] John Justin, Manimurugan S, "A survey on Various Encryption Techniques", IJSCE ISSN: 2231-2307, Volume 2 Issue 1, March 2012.

[3] W Bender, D Gruhl, N Morimoto, "Techniques for Data Hiding", IBM System Journal, Volume 35 No 3, 4, 1996

[4] Ross J Anderson, Fabien A.P.Petitcolas, "On the Limitations of Stenography" IEEE Journal of selected area in communications, ISSN: 0733-8716, May 1998

[5] Gurpreet Kaur, Kamaljeet Kaur, "Digital watermarking And Other Data Hiding Techniques", IJITEE, ISSN: 2278-3075, Volume 2, Issue 5, 2013

[6] E Lin, E Delp, "A Review of Data Hiding In Digital Images", CERIAS Tech Report 2001-139

[7] Hardikkumar V Desai, "Steganography, Cryptography, Watermarking: A Comparative study" JGRCS ISSN: 2229-371X Volume 3, No12, Dec 2012

[8] Gary C Kessler "An Overview of Cryptography" – http://www.garykessler.net/library/crypto.html

[9] Mehdi Hussain, Mureed Hussain, "A survey of Image Steganography Techniques" IJAST Volume 54, May 2013