International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 242-246 www.ijaem.net ISSN: 2395-5252

A Survey on different Data hiding techniques for Secure Image transmission

Richa Sharma[1], Suman Sharma[2], Kriti Sharma[3]
[1]*Assistant Professor, ECE Department, Swami Keshvanand Institute of Technology, Management and Gramothan, Jaipur*
[2]*Assistant Professor, IT Department, Swami Keshvanand Institute of Technology, Management and Gramothan, Jaipur*
[3]*Assistant Professor, IT Department, Arya College of Engineering & IT, Jaipur*

Date of Submission: 10-10-2020 Date of Acceptance: 27-10-2020

ABSTRACT— Digital media processing enables the easy distribution of different kind of media with easy communication means. The easy distribution of digital media leads to unlimited copying as well as unauthentic copying or theft of digital media. Embedding the digital objects in the multimedia data reserves the authentication rights to the content provider.
In digital media processing there are a number of ways to hide some secret digital information in some other media. Cryptography, Steganography and Watermarking are the three well known techniques serving the authenticity of original content.
Keywords— Cryptography, Data hiding, Digital Media, Watermarking**,** Steganography

I. INTRODUCTION

Due to the pervasive nature of the digital multimedia contents, the privacy and security of data has become a major challenge in this digital era. The growth of internet and advances in technology have discovered means of new business, scientific, entertainment and social options in the form of electronic publishing and advertising, real-time information delivery, multimedia sharing, online ordering, transaction processing, digital libraries, web newspapers and magazines, and a lot more. The ease with which people can access, copy and manipulate the multimedia content, has created threat to innovations of publishers, authors and artists. The digital media consists of image, audio and video files which are transmitted over open public network and therefore it is required to protect digital content.

As a valuable solution to the above problem, the ownership data can be embedded within the multimedia file and can be extracted later to identify the owner. Cryptography, Steganography and Watermarking are the three well known techniques serving the authenticity of original content.

II. CLASSIFICATION OF DATA HIDING TECHNIQUES

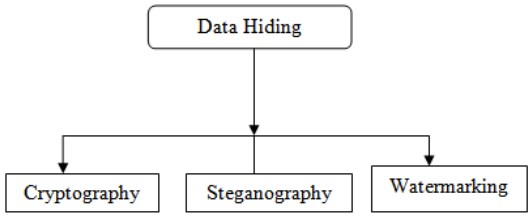

Fig 1. Classification of Data Hiding Techniques

2.1 Watermarking

Watermarking refers to the technique of hiding the secret information in some cover media (e.g. image, audio, video etc.) so that it is not detectable to anyone. Digital watermarking is today's modern solution considered by researchers for preventing unauthorized use, by inserting information, digital watermark, into the original digital data. In case of multiple claims, that embedded watermark plays the key role [1]. The owner of the original data proves his ownership by extracting his previously embedded watermark from the watermarked content. Also the embedded data can effectively be used in protecting data contents from illegal interferences. Usually, the information which is to be embedded could be a logo, a secret data, a meaningful message, or a random signal. In Watermarking, possible cover media could be an image, audio, video, text, signature or some other digital media which will conceal the secret information.
A standard Watermarking scheme adapted by any multimedia data is shown in fig.2.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 242-246 www.ijaem.net ISSN: 2395-5252

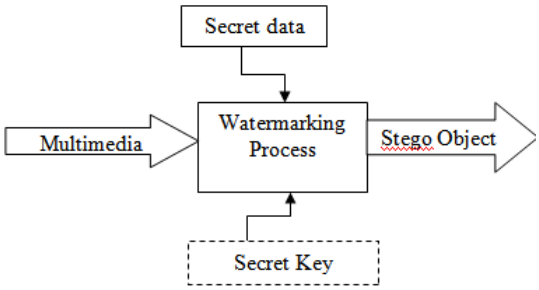

Fig. 2. Basic Watermarking Process

The watermark must have following characteristics.

i. The watermark must not be visible as whole or partially by performing any small alteration over the image.
ii. The watermark must be irremovable after performing any extraction approach; if the watermarking object is removed then the image distortion should be there.
iii. The object must be distributed over the image; it should not be scaled to a particular part over the image.
iv. After the Watermarking, the result image must be feasible under the MSE and PSNR calculation.
v. The pixel modification should not be regular; it must be respective to the image intensity.

III. STEGANOGRAPHY

Watermarking and steganography differ in a variety of ways. The basic difference is that the major entity to be transmitted in watermarking is the host multimedia, embedded data only provides the copyright protection. This embedded data is always associated with the cover multimedia or its owner. While, in Steganography the major entity to be communicated is the embedded message itself, and the cover multimedia serves as an appropriate inoffensive mask chosen by the user [2]. The embedded data could be anything. The essential requirement for Watermarking is that algorithm should be undetectable. However, stegnography is mainly concerned with the robustness against malicious attacks [5]. Steganographic communications between sender and receiver are usually point-to-point. On the other hand, watermarking techniques are usually one-to-many

IV. CRYPTOGRAPHY

Cryptography is defined as an art of secret writing. The word cryptography is derived from the Greek words kruptos (secret, hidden) and graphen (writing). Cryptography involves two processes namely encryption and decryption. Encryption is the process of translating ordinary information referred to as plaintext into unintelligible text referred to as cipher text. Decryption is the reverse process, i.e. converting back the unintelligible cipher text to plaintext. A pair of algorithms that generates the encryption is controlled by cipher and the reversing decryption is normally controlled by a key [3].

Watermarking is often confused with cryptography; these two areas are similar in the way that they are used to protect confidential information. However, the difference between two is that the cryptography keeps the contents of the information secret while Watermarking not only keeps the contents of information secret but keeps the very existence of the information secret. The output of Watermarking operation is not apparently visible but in cryptography the output is scrambled in such a way that it can easily draw the attacker's attention.

V. ATTACKS ON DIGITAL WATERMARKING

Like any other circulating digital media, hided content may be processed in some way before it reaches the receiver. Such processing modifies the content either intentionally or non-intentionally.

In data hiding terminology, an attack can be defined as any processing that may harm or impair thedigital media. Therefore, any processed watermarked data is called attacked data and the processing itself is called an attack [4].

Some of the most common attack categories are given as under:-

i. Removal Attacks

The main aim of these attacks is the complete removal of the information from the transmitted content, without the need to crack the security of the data hiding algorithm.

ii. Geometrical Attacks

Geometrical attacks mainly based on the geometric transformations, which aims at modifying the spatial relationships between pixels of an image.

a. Flipping

Flipping is the geometrical transformation in which a plane figure is flipped or reflected across a line, that creates a mirror image of the original figure. The line of reflection or axis of reflection is the line across which the figure is reflected. If the line of reflection is the x-axis, then it is horizontal

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 242-246 www.ijaem.net ISSN: 2395-5252

flipping, and, if the line of reflection is the y-axis, then it is a vertical flipping.

b. Rotation

In Rotation, a figure is turned about a fixed point. Centre of rotation is that fixed point around which the figure is rotated. Angle of rotation is the degree to which the figure is rotated.

c. Scattering

Scattering is the transformation which aims at separating selected regions of the image and swapping them with other regions of the same image, in different directions.

d. Warping

Image warping is a transformation that defines how each point in the source image should be translated to produce the warped image, thus it changes the spatial configuration of an image.

e. Skewing

Skewing is the act of making a rectangular image slanted so that it can be accomodated into a parallelogram instead of a rectangle.

iii. Cryptographic Attacks

These attacks aim at cracking the security methods those were employed in data hiding schemes. One example of these attacks is brute-force search; it tries to find the embedded secrete information and targets the position where the watermark is inserted . Another most common attack falling under this category is the so-called oracle attack. When the watermark detector device is available, oracle attack can be used to create a non-watermarked signal from the watermarked one. Due to their high computational complexity, the application of these attacks is limited and restricted.

VI. IMAGE PROCESSING FILTERS

Filters in image processing are usually used to smoothen the image, or for enhancement or detection of edges in the image. Following are the filters that are used in in image processing:

i. Random Jitter

It performs a displacement at each pixel position by a random amount, which is given according to an arbitrary distribution.

Each pixel displacement is followed by an interpolation over the modified sampling grid.

ii. Average Filter

It is usually used for smoothing images. The main idea of using this filter is to simply replace each pixel value in an image with the mean or average value of its neighbouring pixel, including itself.

iii. Disk Filter

It is a circular averaging filter, which is based on the average Motion Filter: It is a smoothing filter, and approximates the linear motion of a camera. This can only be achieved by blurring in a single direction.

iv. Gaussian Filter

Gaussian Filter is a 2-D convolution operator which is used to blur images and remove noise from the image..

v. Laplacian Filter

Laplacian filter measures the 2nd spatial derivative of an image. The image Laplacian highlights the regions of rapid intensity change. This filter is used mainly for edge detection.

vi. Log Filter

This filter is the Laplacian of Gaussian filter. A Gaussian smoothing filter smoothes the image and then the Laplacian filter is applied for reduction of sensitivity to noise.

vii. Prewitt Filter and Sobel Filter

Both are used for edge detection. It computes an approximation of the gradient of the image intensity function. This requires convolving the image with a small, separable, and integer valued filter in both horizontal and vertical direction.

viii. Un-sharp Filter

This filter is mainly a sharpening operator, which enhances edges and other high frequency components in an image involving a procedure, which subtracts a smoothed version of an image from the original image..

The size of the filter usually takes a value from the discrete interval [0, max], where the filter of size=0 has no effect on the target image, and the filter of size =max is the filter which destroys the target image completely. We can determine percentage of destruction at the filtered image by comparing it to the original un-filtered image.

VII. DATA HIDING APPLICATIONS

i. Copyright Protection (CP):

Because traditional copyright notices, such as "©", "date", and "owner" are easily removed from the digital content when it is copied; and because copyright notices may cover important portions of the image; watermarking of digital images is used for Copyright Protection instead. The owner of the image's content can be identified by using a hidden object, which is imprinted into the image. The

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 8, pp: 242-246 www.ijaem.net ISSN: 2395-5252

watermark here, allows content's owners to trace their contents and to detect unauthorized use or duplications of it.

ii. Secret Communication :

With the demand for speed over the Internet and advancement in technology, there is always a need for secrecy and private communication [6]. Cryptography is increasingly used for secure communication, where a security key is used, which is shared between participates and watermarking is used for secure communication, to protect data from illegal interferences.

iii. Feature Tagging:

Many descriptive elements like captions, annotations, time stamps can be embedded inside an image. Also the names of individuals in a picture or locations in a map can also be embedded.. In the database of an image, keywords are embedded to facilitate the main search engines. If the image is normally a frame of a video sequence, so for synchronization with audio, timing markers can be embedded in the image.

VIII. CHARACTERISTICS OF DATA HIDING TECHNIQUES

Several parameters have to be considered while evaluating a given data hiding technique [7]. These parameters are:

i. **Invisibility** – The invisibility of a data hiding algorithm is the first and primary requirement, since its lies in its ability to be unnoticed by the human eye [8]. The technique being employed should not be detectable by either naked human eye or by statistical tests.

ii. **Payload Capacity** - Payload Capacity refers to the amount of data bits that can be hidden in the cover medium. Only a small amount of copyright information is embedded in the watermarking process, whereas Steganography process aims at hidden communication therefore it requires sufficient embedding capacity [9].

iii. **Robustness** – All the data hiding algorithms should be robust against either malicious or unintentional image manipulation such as cropping or rotating the image and image filters.

iv. **Independent of file format** – Using only one type of file format continuously for communication between two parties arise a suspicion [9]. Thus a powerful steganographic algorithm should possess the ability to embed information in any type of file format.

v. **Other Characteristics**: Computational complexity of encoding and decoding is another consideration and individual applications may have additional requirements. For instance, form having a copyright protection, a watermark should be resistant to different collusion attacks where many attackers work together to identify and destroy the watermark.

Performacr Evaluation Of Data Hiding Algorithm

i. **PSNR Value** - It is the measurement of the quality between the cover image and Watermarked-image. The larger PSNR value means there is only small difference between the cover-image and the Watermarked-image. On the other hand, a smaller PSNR value means there is huge distortion between the cover-image and the Watermarked-image. Watermarking algorithm aims at providing a large PSNR value.

ii. **MSE Evaluation** – It is the measurement of the performance of the algorithm embedding data in different images and measuring image degradation. Degradation is measured by mean squared error (MSE) between the cover and the Watermarked-image. The better the Watermarked image quality is the lower the MSE value will be [10].

iii. **Normalized Cross Correlation (NCC):** NCC is an important performance parameter in any extracting module. Sometimes, it is needed to have a robust algorithm. The robustness and imperceptibility of a watermarking system is often verified by using NCC by expressing the comparability between the extracted watermark and the original watermark quantitatively.

iv. **Embedding capacity (EC) :**It is a measure to determine the ratio of information that can be embedded in the host image

IX. CONCLUSION

This study presented the different data hiding techniques for secure image transmission. The basic methods and processes of the information hiding system are discussed in this study. The major features of data hiding techniques are reviewed with respect to visual quality, capacity, PSNR, robustness and security. Different attacks and the common image processing filters that can be applied on images are then discussed. Also it can be seen from the discussion that it is important for a data hiding technique to make the embedded data imperceptible.

REFERENCES

[1]. M. Abdullatif, A. M. Zeki, J. Chebil, T. S. Gunawan, "Properties of digital image watermarking", IEEE 9th ICSPA, Kuala Lumpur, pp. 235-240, March 2013.

[2]. A. Cheddad et al.: "Digital image Steganography: Survey and analysis of current methods", Signal Processing, Elsevier, 90(2010) 727-752

[3]. Fabien A.P. Petitcolas et al., "Information Hiding – A survey", Proceedings of IEEE, SpecialIssueonprotection of multimedia content, 87(7): 1062-1078, July 1999.

[4]. M.D. Swanson et al., "Robust Data hiding for images", 7th Digital Signal Processing Workshop (DSP 96), pp. 37-40, IEEE, Loen, Norway, Sep. 1996

[5]. MamtaJuneja and Parvinder Singh Sandhu, (2013)"ANew Approach for Information securityusinganImproved Steganography Technique",Journal of Info. Pro. Systems, Vol 9, No:3, pp.405

[6]. N. F. Johnson and S. Katzenbeisser, "A Surveyofsteganographic techniques.in Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, (2000), pp. 43-78

[7]. M. J. Anwar, M. Ishtiaq, M. A. Iqbal, M. A. Jaffar, "Block-based digital image watermarking using Genetic Algorithm", 6th International Conference on Emerging Technologies, pp. 204-209, October 2010.

[8]. L. M. El Bakrawy, N. I. Ghali, A. ella Hassanien, Tai-hoon Kim, "A rough k-means fragile watermarking approach for image authentication", Federated Conference on Computer Science and Information Systems,Szczecin, pp. 19-23, September 2011.

[9]. D. M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," IEEE Transactions on Image Processing 3, pp. 721-730, Mar. 2007.

[10]. J. Tian, "Reversible data embedding using expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, Aug. 2003