International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 4, July-Aug-2018, ISSN (Online): 2395-566X

A Survey on Robust Image Watermarking Techniques and Different Applications

M.Tech. Scholar Kanchan Sahu
Dept. of Computer Science
Sri Balaji Institute of Tech. & Management
Betul, MadhyaPradesh, India
E-mail- Kanchan.sahu1426gmail.com

Asst.Prof. Pravin Malviya
Dept. of Computer Science
Sri Balaji Institute of Tech. & Management
Betul,MadhyaPradesh,India
E-mail-malviyapravin2010gmail.com

***Abstract* – Image Watermarking is used for copyright protection, authentication and ownership of the intellectual property. Visual cryptography is technique in which secret data is decomposed into number of shares and distributed to participants, So that only participants can read that data. Image Visual Cryptography is used to keep the data private from unauthorized users. Here detail survey of different image watermarking techniques used by various researcher are detailed. Various properties of the image data hiding was explained.**

***Keywords*-Color Format, Digital Watermarking, Frequency domain, LSB etc.**

I. INTRODUCTION

The growth of the digital multimedia technology and the successful development of the Internet have not only allowed people to process, deliver and store digital content more easily, but also have gifted the facility of copying it rapidly and perfectly without loss of quality, with no limitation on the number of copies, tempering with and redistributing illegally without authorization.

This kind of advantages raises the issue of how to protect copyright ownership of digital data. Cryptography is not a solution, because data after decryption can always be distributed in plain form without any restriction, even by the authorized customer. A better solution to this problem is to integrate the security information directly into the content of the digital data in inseparable form during its useful lifespan, and digital watermarking is such an effective way to protect copyright of the digital multimedia data even after its transmission.

Watermarking is the process that enables data called a watermark, digital signature, tag, or label into a multimedia object such as audio, image or video in perceptually invisible or inaudible manner without degrading the quality of the object, such that watermark can be detected or extracted later to make an assertion about the object [1-4].

The embedded information can be a serial number or random number sequence, ownership identifiers, copyright messages, control signals, transaction dates, information about the creators of the work, bi-level or gray level images, text or other digital data formats [5].

Digital watermarking gives value-added protection on the top of data encryption and scrambling for content protection and effective digital rights management [6]. Typically watermark contains information about the origin, ownership, destination, copy control, transaction etc. Watermarking has many different applications such as copyright protection, transaction tracking, copy control, ownership identification, authentication, forensic analysis, playback screening, legacy system enhancement and database linking etc [7-9].

Copyright protection of digital data is defined as the process of proving the intellectual property rights to a court of law against the unauthorized reproduction, processing, transformation or broadcasting of digital data [7]. It can embed information about the owner of the object, which can be used for resolving rightful ownership.

Each digital object has a unique watermark identifying the buyer of the object, which requires a very high level of robustness for fingerprinting for traitor tracking so that buyers can be trace. For copyright-related applications, the embedded watermark is expected to be robust to various kinds of malicious and non-malicious attacks, provided that the manipulated content is still valuable in terms of perceptual quality [10].

Although some significant progresses have been done recently, one of the major problems in the practical watermarking methods is the insufficient robustness of the existing watermarking algorithms against geometrical attacks such as sharpening, lightening,

darkening, cropping, blurring, distorting, scaling, jittering, rotation and, removal attacks such as denoising, quantization, remodulation, filtering, JPEG compression, collusion, print-copy-scanning, cryptographic attacks and protocol attacks. Majority of geometrical and removal attacks come under malicious attacks. Malicious attacks attempt to remove or disable watermark [11].

II. RELATED WORK

In [7] Miss. Kashmira S. Gulhaneet al (2016) In this paper the Image is divided into parts known as shares and then these shares are distributed to the participants. In Decryption phase stacking the share images gets the original image. For the RGB/CMY Images different methods are developed which are based on the color decomposition techniques. The Decryption process is very easy generated shares are printed on transparencies.

Transparencies are overlapped on top of the other gets the secret image. The displacement of pixels and rearranging of the image in steps between the processes has proven to be valuable. The extra transposition of RGB values in the image file after RGB component reshape has proven to increase the security of the image against all probable attacks available currently.[10]

In [3] Kalyan Daset al (2016) In this paper they have applied Sliding Puzzle Technique on the images and showed good result without any alteration. The algorithm proposed by this scheme reduces the time for encryption and decryption of images in a much easier way and it ensures the lossless transmission of images. Encryption is carried out on the basis of RGB values of pixels. Hybrid approach to visual cryptography where they take colored images and split the image into multiple rows and columns, resulting image tiles. For decryption, they have (row*col)! Combinations out of which only one gives back the original image. For this purpose symmetric key is used.

In [5] NidhalKhdhair El Abbadiet al (2016) In this paper they suggested a new method of image encryption based on three major steps: the first step aims to scrambling the image values with Fibonacci transform. The second step aims on generating public and private key based on Diffie-Hellman key exchange, these keys used to encrypt the diagonal matrix which are formed by (SVD) Singular Value Decomposition .

In third step, decryption is the contrary to encryption. The results were assured and the decrypted image is retrieved without any loss in its information.

In [4] K.Kanagalakshmet al (2016) In this paper they proposed a method that is based on Blowfish algorithm with superior features. It has been enhanced with the help of a supplementary key approach to strengthen the security of image or any sensitive data which are communicated by electronic means. The proposed algorithm is developed and tested with different sets of data. The performance of the proposed methods is considered in terms of time, space complexity and security also. The results are recorded and a better performance is observed.

In [2] Gaurav Kumar et al (2016) In this paper they have purposed a new technique known as digital watermarking as the simple visual cryptography is not so secure for sharing of data and it also does not ensure the user authentication. In this cryptographic technique secret images are divided into n shares and a certain number of shares (m) are sent over the network. This project presents an approach in which visual cryptographically generated image shares are embedded in the host images to provide authentication for the VC shares and makes these secret shares invisible by embedding them into host images.

The shares are embedded into the host image in Frequency Domain using Discrete Cosine Transform (DCT).The weakness of binary secret shares is overcome by hiding them invisibly into the host images. In decryption phase, the secret shares are extracted from their cover images without need of any cover image characteristics because the watermark extraction scheme is blind. The overlapping of these shares reveals the original secret image. The decoded secret image quality is enhanced.

In [8] AshaBhadran R(2015) Inthis paper presents a visual cryptography technique for color images in which the generated shares are again encrypted. For this XOR operation is used and this will provide double security for the secret document. Secret shares are not available in their actual form for any modification by the adversaries who try to create fake shares. The proposed method uses the concept of half toning. When the color image is given as input, decoded image was color halftone image.

In [9] M.Karolinet al (2015) In this paper they proposed a method for images with 256 colors which are converted to 16 standard RGB colors format. It generates shares without compromise the resolution. The Floyd – Steinberg dithering algorithm is used to manipulate the 256 color code image to decrease it to 16 standard colors code image. The proposed method employs (2, 2) XOR-Based visual cryptography method is used to generate shares. Decryption procedure enables secret image sharing and stacking.

The proposed method converts the 256 color image to 16 color code format for the share formation, the intensity of the original image is maintained.
In [11] Manika Sharmaet al (2013) Inthis paper they proposed a cryptographic technique for color images where we are using color error diffusion with XOR operation. To add more security to the secret sharing of the image Invisible Digital Watermarking is used which protects the secret image from the hacker. Random number procedure is used to generate the shares.In decryption process use RSA algorithm. This approach produce a reduced amount of unclear image and the size of the decrypted image is equivalent as the original image.

III.PROPERTIES OF WATERMARKING

Watermarking need some desirable properties based on the application of the watermarking system [2]. Some of the properties are presented here:

- Effectiveness: This is the most important property of watermark that the watermark should be effective means it should surely be detective. If this will not happened the goal of the watermarking is not fulfilled.
- Host signal Quality: This is also important property of watermarking. Everybody knows that in watermarking, watermark is embedded in host signal (image, video, audio etc.). This may put an effect on the host signal. So the watermarking system should be like as, it will minimum changes the host signal and it should be unnoticeable when watermark is invisible.
- Watermark Size Watermark is often use to owner identification or security confirmation of host signal and it always use when data is transmitted. So it is important that the size of watermark should be minimum because it will increases the size of data to be transmitted.
- Robustness Robustness is crucial property for all watermarking systems. There are so many causes by which watermark is degraded, altered during transmission, attacked by hackers in paid media applications. So watermark should robust, So that it withstand against all the attacks and threats.

IV. TECHNIQUES OF WATERMARKING

1. Spatial domain- Spatial domain digital watermarking algorithms directly load the raw data into the original image [3]. Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. Spatial domain is manipulating or changing an image representing an object in space to enhance the image for a given application. Techniques are based on direct manipulation of pixels in an image [10]. Some of its main algorithms are as discussed below:

2. Additive Watermarking- The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or sometimes floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of different keys will be very low [10].

3. Least Significant Bit-Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image. But these primitive techniques are vulnerable to attacks and the watermark can be easily destroyed. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications.

4. SSM Modulation Based Technique-Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.
5. Texture mapping coding Technique-This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage) [3], and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture.

6. Patchwork Algorithm-Patchwork is a data hiding technique developed by Bender et alii and published on IBM Systems Journal, 1996[11]. It is based on a pseudorandom, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is carried out where the first one is A and the second is B. Patch A image data is brightened where as that of patch B is darkened (for purposes of this illustration this is magnified).

7. Frequency domain- Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients [13].

V.APPLICATIONS OF WATERMARKING

Watermarking technologies is applied in every digital media whereas security and owner identification is needed[3]. A few most common applications are listed hereby.

- Owner Identification The application of watermarking to which he developed is to identify the owner of any media. Some paper watermark is easily removed by some small exercise of attackers. So the digital watermark was introduced. In that the watermark is the internal part of digital media so that it cannot be easily detected and removed. 3.2.2 Copy Protection illegal copying is also prevent by watermarking with copy protect bit. This protection requires copying devices to be integrated with the watermark detecting circuitry.
- Broadcast Monitoring Broadcasting of TV channels and radio news is also monitoring by watermarking. It is generally done with the Paid media like sports broadcast or news broadcast.
- Medical applications Medical media and documents also digitally verified, having the information of patient and the visiting doctors. These watermarks can be both visible and invisible. This watermarking helps doctors and medical applications to verify that the reports are not edited by illegal means.
- Fingerprinting A fingerprinting is a technique by which a work can be assigned a unique identification by storing some digital information in it in the form of watermark. Detecting the watermark from any illegal copy can lead to the identification of the person who has leaked the original content. In cinema halls the movies are played digitally through satellite which has the watermark having theater identification so if theater identification detected from a pirated copy then action against a theater can be taken.
- Data Authentication Authentication is the process of identify that the received content or data should be exact as it was sent. There should be no tampering done with it. So for that purpose sender embedded the digital watermark with the host data and it would be extracted at the receivers end and verified. Example like as CRC (cyclic redundancy check) or parity check.

VI.CONCLUSION

In today's world security of the image is very important. In this paper we have surveyed different problems and techniques in the years. As conclude that all techniques are good for data hiding and have their own advantages and disadvantages and give a security so that no one can access the image in open network. It has been observed that during extraction watermark is the main focus of most of the researcher but few of them work on original image as well but reverse process of both watermark and original image is still not done. Watermark is mainly compare on the basis of the attack but most of the paper work on the spatial attack and show effective results in various attacks with different levels. A unique algorithm is still reuired which focus on both watermark and original image with high robustness against spatial as well as geometric attacks.

REFERENCES

[1]. Mohammed A. M. Abdullah, Satnam S. Dlay, Wai L. Woo, and Jonathon A. Chambers. "A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography". IEEE Access Year: 2016, Volume: 4 Pages: 10180 – 10193.

[2]. Gaurav kumar, Sachin chaudhary, "A Visual Cryptography scheme to secure black and white image shares using Digital Watermarking " in IJARCSSE, Volume 6 Issue 5, May 2016.

[3]. Kalyan Das, Aromita sen, Samir kumar Bandyopadhyay" A new Visual Cryptography scheme for color images using sliding puzzle technique" in IJIRR, Volume 03, Issue 04,April 2016.

[4]. K.Kanagalakshm, M.Mekala, "Enhanced Blowfish algorithm for image encryption and decryption with supplementary key "in IJCA, Vol. 146-No 5,July 2016.

[5]. NidhalKhdhair El Abbadi, Samer Thaaban Abbas, AliAbd Alaziz, "New image encryption algorithm based on Diffie – Hellman and Singular value Decomposition " in IJARCCE, Vol. 5, Issue 1, January 2016.

[6]. Monika Bhosale, RajshreeChaudhary, PrathameshGaddam, AyushiKedarYogesh. J.Pawar, "Visual Cryptography Scheme for Secret Image Retrieval", Vol. 3,Issue 3 March 2016.

[7]. Miss. Kashmira S. Gulhane,Prof. P.L.Ramteke,"VISUAL CRYPTOGRAPHY USING IMAGE"in IJRISE, Vol. 2, Issue 1,2016.

[8]. AshaBhadranR,"An Improved Visual Cryptography Scheme for colour images" in IRJET, Aug-2015, Vol. 2, Issue No.5.

[9]. M.Karolin, Dr. T. Meyyapan,"RGB based secret sharing scheme in color Visual Cryptography",in IJARCCE, July 2015 vol. 4,Issue No. 7.

[10]. Dilip Kumar Mishra, P.G.Scholar, Sriram Yadav. "Chaotic Function Based Data Hiding Approach at Least Significant Bit Positions".. www.ijsret.com IJSRET Volume 4 Issue 1, January-2018

[11]. Manika Sharma, RekhaSaraswat, "Secure Visual Cryptography technique for color images using RSA algorithm", in IJEIT,April-2013, Vol. 2, Issue No.10.