A Survey on Digital Watermarking for Image Authentication

Mrs. C. Christy,
Assistant Professor,
P.G. & Research Department
of Computer Science,
St. Josephs' College of Arts
and Science – Cuddalore.
Tamilnadu.

Mr. A. Baskaran,
M.Phil. Research Scholar,
P.G. & Research Department
of Computer Science, St. Joseph's
College of Arts
and Science – Cuddalore.
Tamilnadu.

Mr. P. Arunmani,
M.Phil. Research Scholar,
P.G. & Research Department
of Computer Science,
St. Joseph's College of Arts
and Science – Cuddalore.
Tamilnadu.

***Abstract*:- The aim of this paper is to discuss the importance of Digital Watermarking for copyright protection and authentication of multimedia data. By the use of cryptography keys the watermark should be general in secret and accessed by only through authorized persons. Embedding and Extraction process can be handled to watermark the host image. Depending on the application,watermark provides remarkable information. One or more crypto graphical key should be used. The basic idea behind watermarking is to add a watermark signal to the host data to be watermarked and the watermark signal is unremarkable. Watermark is a digital code that imperceptibly, robustly embedded in the host data. There are three different watermarking multimedia techniques are available such that text, image and video.**

Keywords: Copyright, imperceptibly, robustness, signal, Embedding, Extraction.

I.INTRODUCTION

The rapid and extensive growth in Internet technology is creating a pressing need to develop several newer techniques to protect copyright, ownership and content integrity of digital media. This necessity arises because the digital representation of media possesses inherent advantages of portability, efficiency and accuracy of information and also puts a serious threat of easy, accurate and illegal perfect copies of unlimited number. Unfortunately the currently available formats for image, audio and video in digital form do not allow any type of copyright protection.

A potential solution to this kind of problem is an electronic stamp or digital watermarking which is intended to complement cryptographic process. While the later technique facilitates access of the encrypted data only for valid key holders but fails to track any reproduction or retransmission of data after decryption. In digital watermarking, an identification code (symbol) is embedded permanently inside a cover image which remains within that cover invisibly even after decryption process.

The aim of watermarking is to include hidden information (i.e., imperceptible) in a multimedia document to ensure a security service or simply a labelling application. It would be then possible to recover the embedded message at any time, even if the document was altered by one or more non-destructive attacks, whether malicious or not.

Furthermore, it is generally impossible to tell whether a given image is authentic or has been altered subsequent to capture by some readily available digital image processing tools. This is an important issue for legal applications, news reporting and medical archiving, where it is sure that the digital image truly reflects the scene looked like at the time of capture.

Another need of image authentication arises in electronic commerce where the seller transmits a digital image to the buyer who wants to be sure that the received image is indeed genuine. Here verification of the integrity of an image alone is not sufficient, but the ownership must also be checked. Therefore it is necessary to insert a watermark into an image for authentication and integrity.

The objective of this project work is to design and implement a watermarking scheme for image authentication. For uncompressed images, an invisible watermark is embedded through LSB technique in the spatial domain. It is only possible for someone who has ownership of a valid user key to check the ownership, while someone who does not have a valid user key will not be able to forge a watermark. For compressed image, an invisible watermark is embedded via table look-up in the frequency domain. This technique is suitable only for compressed images.

Watermarking is the process of embedding data into a multimedia element such as image, audio or video. This embedded data can later be extracted from, or detected in, the multimedia for security purposes. A watermark can be visible or invisible depending upon the desire of the user. Visible watermark appears visible to a casual viewer on a careful inspection and it is easily detected by observation. While an invisible mark is designed to be transparent to the observer and embedding in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism. There are two different ways of embedding invisible information in a digital image.

- In the spatial domain
- In the transform domain

II. BASIC DOMAINS

- SPATIAL DOMAIN

Spatial domain embeds directly in the image pixel data. By some image analysis operations (e.g. Edge detection), it is possible to get perceptual information about the image, which is then used to embed a watermarking key, directly in the intensity values of encoded regions of the image. It provides a simple and effective way for embedding an invisible watermark into an original image but doesn't show robustness to common image alterations.

- TRANSFORM DOMAIN

In this transform domain, first transforming the original image into the frequency domain by the use of Fourier, Discrete Cosine or Wavelet transforms. With this technique, the marks are not added to the intensities of the image but to the values of its transform coefficients. Then, inverse-transforming the marked coefficients form the watermarked image. The use of frequency based transforms allows the direct understanding of the content of the image.

In general, watermarking technique needs to possess the following characteristics:

1. Imperceptibility for hidden information.
2. Redundancy in distribution of the hidden information inside the cover image to satisfy robustness in watermark extraction process even from the reduced (cropped) watermarked image.
3. Possible use of one or more keys to achieve cryptographic security of hidden content.

Besides these general properties, an ideal watermarking system should also be flexible to insertion of additional watermarks to retain the rightful ownership.

III. RESEARCH SO FAR

Major Contribution and Research work in Digital Watermarking:

Digital water technique has been explained as a [1] newly frequency domain is introduced for digital watermarking by arranging the set of real numbers in a normal distribution of DCT co-efficient in a zigzag scan like as in the JPEG algorithm.

In this paper [2] Hash block chaining version is used to secure instead RSA and public key weakness in fragile authentication. Several attacks such as birthday attack made for robustness.
Watermarking techniques [3] introduces a novel DWT – SVD perceptual fidelity metric for watermarking scheme evaluation. Several image distortion metrics is validated through subjective assessment.

Many research techniques involved [4] due to robustness in watermark in signal processing such as lossy compression, filtering, digital to analog,etc. It provides that the transformed image registered. Tamper – resistant algorithms were used for electronic watermarking.

A SVD based image authentication [5] introduced against various vector attacks with improved security. JPEG compression robustness verified by block wise quantization based embedding.

In this paper [6] Proposed watermarking methods for images, audio, video and text documents. A watermark typically host data and application include copyright protection, data monitoring and data tracking.

Digital watermarking techniques [7] visually recognizable patterns for embedding the watermark. Secret information will be hided in the digital image. DCT based watermarking with embedding and extraction procedure.

In this paper [8] ICA (Independent Component analysis) algorithm used for extraction which takes the advantage of image signature without reducing the payload of the real watermark. To reduce the copy attack, an image dependent signature is applied and embedded.

Watermarking algorithms [9] Combining both embedding strategy and features of HVS, an algorithm adaptive to it. Embedding formula should be applied Texture masking and luminance masking of the human visual system.

In this paper [10] A technique with JPEG lossy compression but prevents malicious manipulations. Thus the image authentication customize to accommodate different requirements and “desirable” manipulations. Separate blocks of an image is based on the relationships between discrete cosine transform (DCT) coefficients.

For an effective watermarking [11] SVD (Single value decomposition) uses non fixed orthogonal bases. It’s based on one way non symmetrical decomposition. First, watermarking protect rightful ownership to provide trustworthy. Filtering, compression resist distortions satisfy robustness.

In this paper [12] Based on the Chinese Remainder Theorem, generalization APM-LDPC codes permutation matrices present a class of low density parity check(LDPC). Without sacrificing properties, LDPC codes can be generated.

The research in watermarking [13] Advantages of IA-DCT algorithm has an advantage decompressed JPEG bit streams watermarked partially. IA-W scheme based on account frequency sensitivity, the multi resolution. Image adaptive watermarking schemes developed for compression applications using visual models. Block based discrete cosine transform multiresolution wavelet framework were discussed.

Digital watermarking is the solution for [14] safe ownership of digital images, copyright protection and

content authentication. Using least significant bit (LSB) method, watermarking in spatial and frequency domain. The process of embedding a signal is watermarking and the host or cover is the other signal. In addition to the noise cropping LSB performed on gray scale images.

In this paper [15] Computational cost is low by both the extraction and embedding of watermarks are done in the compressed domain. Robust MPEG-2 video techniques proposed. A set of blind watermarking techniques widely used to decrease the bit rate of MPEG-2 including cropping and frame dropping.
Watermarking techniques [16] Authentication and ownership verification we use a watermarking scheme. Secret and public key is used for insertion and extraction procedure. If the correct key is given, then then the output image is authentic otherwise image with random noise appear. Uncompressed images in the spatial domain and compressed images in the transform domain cryptography is more secure.

In this paper [17] Single value decomposition (SVD) followed by Chinese remainder theorem (CRT) is resistant to any kind of attacks. Computational complexity is much less. In the proposed scheme, the TAF is found to be below 10% for JPEG compression. It is very effective and efficient for digital watermark.

Attempts to overcome the problem [18] Cropping and tampering attacks is superior by maintaining the robustness of brightening and the algorithm is sound towards the usage of SVD in watermark ownership and authentication is done through digital watermarking.

IV. WHY WATERMARKING IS BETTER

A Watermarking algorithm consists of the following three parts.

- Watermark
- Encoder (insertion algorithm)
- Decoder and comparator(extraction algorithm)

Let us denote an image by I, a signature by S =s1, s2….. and the watermarked image by Î. E is an encoder function, it takes an image I and a signature S and it generates a new image which is called watermarked image Î, mathematically,

$$E (I, S) = \hat{I}$$

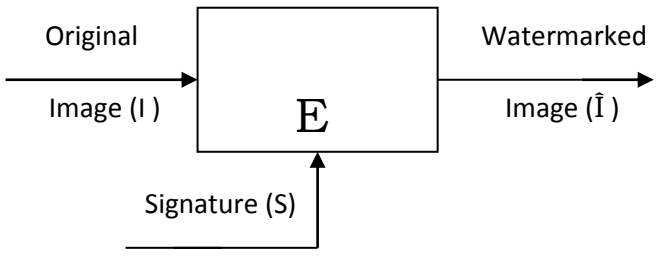

Figure 1. Encoder

A decoder function D takes an image J (can be a watermarked or un-watermarked image, and possibly corrupted) whose ownership is to be determined and recovers a signature S′ from the image. In this process an additional image I can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against planned and accidental corruption of pixels. Mathematically,

$$D (J, I) = S'$$

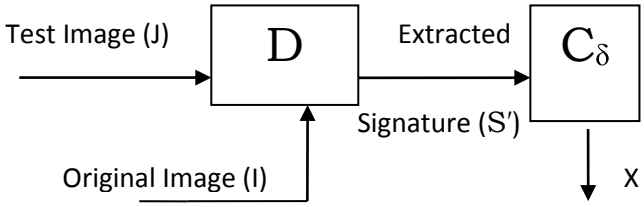

Figure 2. Decoder and Comparator

The extracted signature S′ will then be compared with the owner signature sequence by a comparator function Cδ and a binary output decision generated. If there is match the comparator function returns 1 and 0 otherwise, this can be represented as follows:

$$C\delta (S', S) = \{1, c <= \delta$$
$$\{0, \text{otherwise}$$

Where C is the correlator,

c is the correlation of two signatures and δ is certain threshold. Without loss of generality, watermarking scheme can be treated as a three-tuple (E, D, δ).

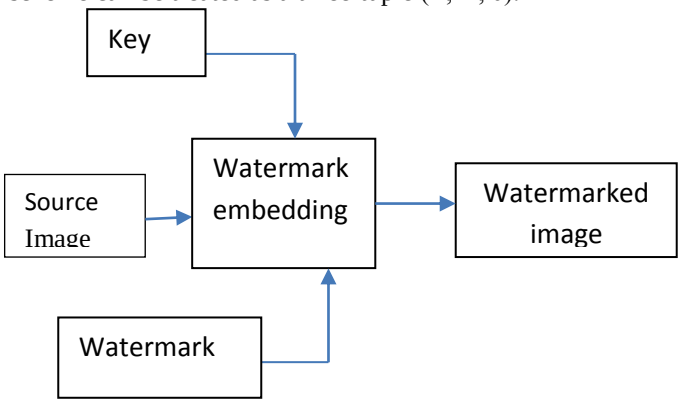

Figure3 :Watermark Embedding Process

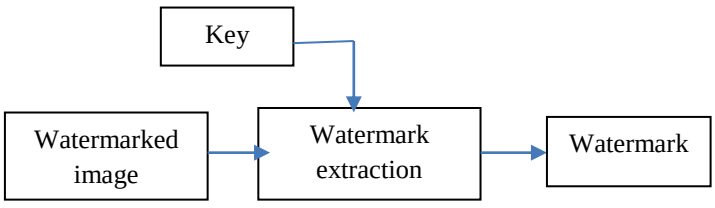

Figure4 : Watermark Extraction Process

V. TYPES OF DIGITAL WATERMARKING

5.1 VARIOUS TYPES

The primary reason for using watermarks is to identify the owner of the content by an invisible hidden "mark" that is imprinted into the image. Watermarking can be categorized into seven types.

- Visible
- Invisible
- Robust
- Fragile/Semi-fragile
- Spatial
- Image adaptive
- Blind

5.1.1 Visible watermarks

Visible watermark is a process that embeds data that is intentionally noticeable to a human observer, in which case their use is two-fold.

- to discourage unauthorized usage
- act as an advertisement

Example of this watermarking is logos used in papers in currencies. It is difficult to remove, rather removing a watermark should be more costly and labour intensive than purchasing the image from the owner.

5.1.2 Invisible watermarks

Invisible watermarks are invisible to a viewer. It will not cause any degradation in the visual quality or in the usefulness of the data. They can be detected and extracted later to facilitate a claim of ownership, yielding relevant information as well.

Example of this type of watermarking is images distributed over the internet with watermarks embedded in them for copyright protection.

5.1.3 Robust Watermarks

Robust watermarks should be stuck to the document. It has been embedded in such a way that any signal transform of reasonable strength cannot remove the watermark and are good for copyright control.

5.1.4 Fragile/Semi-Fragile Watermarks

Fragile watermarks are those that are easily destroyed by any attempt to tamper with them. Absence of a watermark in a previously watermarked document would lead to the conclusion that the data has been alter with.

5.1.5 Spatial Watermarks

These Watermarks are constructed in the image spatial domain, and embedded directly into an image's pixel data. Spectral watermarks are incorporated into an image's transform coefficients.

5.1.6 Image Adaptive Watermarks

These watermarks are usually transform-based, and very robust. They locally adapt the strength of the watermark to the image content through perceptual models for human vision. These models were originally developed for image compression.

5.1.7 Blind Watermarks

These techniques can perform verification of the mark without use of the original image. Other techniques rely on the original to detect the watermark. Many applications require blind schemes; these techniques are often less robust than non-blind algorithms.

VI. ATTACKS ON WATERMARKS

6.1. Active attacks:

The hacker tries deliberately to remove the watermark or simply make it untraceable. This is a big issue in copyright protection, fingerprinting or copy control.

6.2. Passive attacks:

The attacker is not trying to remove the watermark, but simply attempting to determine if a given mark is present or not. The protection against passive attacks is of utmost importance in secret communications where the simple knowledge of the presence of watermark is often more than one wants to grant.

6.3. Collusion attacks:

The goal of the hacker is the same as for the active attacks but the method is slightly different. In order to remove the watermark, the hacker uses several copies of the same data each containing different watermark, to construct a new copy without any watermark. There is a problem in fingerprinting applications (e.g. in the film industry) but is not widely spread because the attacker must have access to multiple copies of the same data and that the number needed can be attractive important.

6.4. Forgery attacks:

The important concept in data authentication is forgery attacks, the hacker aims at embedding a new, valid watermark rather than removing one. By doing so, it allows modifying the protected data as it needs and then, re-implants a new given key to replace the destructed (weak) one, thus making the corrupted image seem real.

A lot of new attacks can be designed and it is impossible to know what will come out next from the hackers' imagination. To those unkind attacks, one must add all signal processing operations involved in the transmission or storage of data, which can naturally degrade the image and alter the watermarked information to the point of not being detectable anymore.

VII. COMPARISON BETWEEN STEGANOGRAPHYVs. WATERMARKING

Steganography is analogous to digital watermarking. It is the art of hiding information in which it prevents detection of hidden messages. Without considering the robustness to hide secret data in digital media by modifying its original but the application is different from watermarking. The main difference between watermarking and steganography is that, in watermarking the cover is the object of communication while in steganography the hidden message is the object of the communication.

VIII. CONCLUSION

- Watermarking has its applications in image/video copyright protection.
- It may be used for certification, conditional access and copy control.
- It is applicable to electronic commerce and World Wide Web.
- Watermarking is mainly used for authentication and ownership identification.
- In order to complete the tracing of image utilization on a distribution media, finger printing is used.

IX. REFERENCES

[1] A. Bariii, F. Bartoliiii, V. Cappellini, A. Piva, I. Elettronica, U. Fireiize, and S. Marta, "ROBUST WATERMARKING OF STILL IMAGES," pp. 499–502.
[2] P. S. L. M. Barreto, H. Y. Kim, and V. Rijmen, "Toward secure public-key blockwise fragile authentication watermarking," vol. 1, pp. 57–62.
[3] F. Del Colle and J. C. G, "A DWT-SVD BASED PERCEPTUAL IMAGE FIDELITY METRIC FOR WATERMAKING SCHEMES."
[4] I. J. Cox, S. Member, J. Kilian, F. T. Leighton, and T. Shamoon, "Watermarking for Multimedia," vol. 6, no. 12, pp. 1673–1687, 1997.
[5] D. Ee, "AN SVD-BASED WATERMARKING METHOD FOR IMAGE CONTENT AUTHENTICATION WITH IMPROVED SECURITY Digital Contents Research Division , ETRI , Daejon , Korea," pp. 525–528, 2005.
[6] F. Hartung, S. Member, and M. Kutter, "Multimedia Watermarking Techniques," vol. 87, no. 7, pp. 1079–1107, 1999.
[7] C. Hsu, J. Wu, and S. Member, "Hidden Digital Watermarks in Images," vol. 8, no. 1, pp. 58–68, 1999.
[8] H. Hu, "Scheme resistant to copy attack," pp. 154–157, 2005.
[9] J. Huang, Y. Q. Shi, and Y. Shi, "Embedding Image Watermarks in DC Components," vol. 10, no. 6, pp. 974–979, 2000.
[10] C. Lin and S. Chang, "Distinguishing JPEG Compression from," vol. 11, no. 2, pp. 153–168, 2001.
[11] R. Liu, T. Tan, and S. Member, "An SVD-Based Watermarking Scheme for Protecting," vol. 4, no. 1, pp. 121–128, 2002.
[12] S. Myung and K. Yang, "A Combining Method of Structured LDPC Codes from Af fi ne Permutation Matrices," no. 1, pp. 674–678, 2006.
[13] C. I. Podilchuk and W. Zeng, "Image-Adaptive Watermarking Using Visual Models," vol. 16, no. 4, pp. 525–539, 1998.
[14] A. K. Singh, N. Sharma, M. Dave, and A. Mohan, "A Novel Technique for Digital Image Watermarking in Spatial Domain," pp. 497–501, 2012.
[15] Y. Wang and A. Pearmain, "Blind MPEG-2 Video Watermarking Robust Against Geometric Attacks : A Set of Approaches in DCT Domain," vol. 15, no. 6, pp. 1536–1543, 2006.
[16] P. W. Wong, S. Member, and N. Memon, "Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification," vol. 10, no. 10, pp. 1593–1601, 2001.
[17] "DCT DOMAIN WATERMARKING SCHEME USING CHINESE REMAINDER THEOREM FOR IMAGE AUTHENTICATION Jagdish C . Patra , Jiliang E . Phua and Deepu Rajan," pp. 111–116, 2010.
[18] "An Improved SVD-Based Watermarking Technique for Image and Document Authentication," vol. 00, no. 2, pp. 1984–1987, 2006.