Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 5, May-2016

Survey on Image authentication based on Reversible watermarking and Perceptual hashing

Ruchika Singh Chandel[1], Rahul Joshi [2]

[1] *IT Department, PIET*
[2] *IT Department, PIET*

Abstract —Accessibility of digital content in this digital era is simpler hence navigates towards a threat for unauthorized access. Vulnerable use of such contents can harm the integrity and confidentiality of data. Reversible watermarking provides the regeneration of original image in addition to watermark. Perceptual hashing supports the multimedia file security in an efficient way. Combination of the above provides efficient, secure and high embedding capacity.

Keywords- Reversible Watermarking, Perceptual Hashing, Image Authentication, Hiding Capacity, Mean Value based Embedding.

I. INTRODUCTION

The art of secretly hiding and communicating information has gained immense importance in the past years due to the advances in generation, storage, and communication technology of digital content. Watermarking is one of the promising solutions for tamper detection and protection of digital content [4]. However, watermarking can cause damage to the sensitive information present in the cover work. Therefore, at the receiving end, the exact recovery of cover work may not be possible. There exist certain applications that may not tolerate even small distortions in cover work prior to the downstream processing. In such applications, reversible watermarking instead of conventional watermarking is employed. Reversible watermarking of digital content allows full extraction of the watermark along with the complete restoration of the cover work. For the last few years, reversible watermarking techniques are gaining popularity because of its increasing applications in some important and sensitive areas, i.e., military communication, healthcare, and law-enforcement. Due to the rapid evolution of reversible watermarking techniques, a latest review of recent research in this field is highly desirable.

In a heterogeneous network, there are servers, clients, and intermediate nodes with different computing capabilities. The distribution chain is not perfectly reliable, due to issues like incidental distortion like format change and malicious modification such as replacing content. In such a circumstance, an important question is whether the received content is authentic. The above problem is easy when the original content is available for comparison, but in practice it is usually not the case. When the original content is not available, a possible solution is to generate a hash value on the server side and send it securely to the client side. The hash value is a compact abstract of the content. A client can re-generate a hash value from the received content, and compare it with the original hash value. If they match, the content is considered as authentic. Conventionally, there exist cryptographic hash algorithms for data authentication, such as MD5, SHA-1. However, they are not suitable for multimedia data, because they are extremely sensitive and do not tolerate any change of the data. In order to correctly authenticate the content even when it has undergone some incidental distortion, the hash value must possess some robustness. Therefore, a new generation of hash algorithms has emerged in the multimedia domain, called robust or perceptual hash (PH) algorithms [8].

Various survey conducted in security field provide the clear view towards research in respective area. In [3] a survey of reversible watermarking techniques based on compression, histogram modification, Quantization and Expansion derives comparison with following parameters fragility, blind and predictor type. A novel prediction error expansion-based reversible image watermarking technique is proposed in [2] which exploits the variance of neighboring pixels in a way that the embedding of information bits in each pixel of an image depends on the scale of variation present in its eight neighboring pixel values. A rhombus predictor is employed in the proposed scheme for its efficacy thus introduces less distortion, good embedding performance, especially at high capacity. In the paper [1], use of quantization module followed by a crypto-compression module is proposed. Randomized feature extractions are made for security against intentional attacks and encryption of image using secret key Secure Hash Algorithm-1(256 bits). In [5] author suggested technique of embedding multiple watermarks by choosing various reversible watermarking methods and using them in combination to perform embedding. They have chosen three methods: 1) Reversible watermarking based on integer transform. 2) High capacity reversible watermarking based on integer transform. 3) Reversible image watermarking using dynamical prediction-error expansion. Pseudorandom codes are used for the secret information to embed. In [7] proposed scheme generates authentication codes by using random number values induced by the selected random number seed. Two set of authentication codes are generated for tamper detection procedure. Cannot detect some modified blocks in the boundary of the tampered area. [9] uses technique: Hashing based on FJLT (Fast Johnson Lindenstrauss

Transform), Watermarking: DCT based blind watermarking. Paper [13] highlights categories of reversible watermarking and their comparison yielding research issues. In [14] arithmetic coding technique is used to compress a part of the original image and store the compressed data together with necessary authentication information as the payload. The payload is then embedded within the original image with consideration of the HVS. Due to this, the watermarked image contains no perceptible artifacts. In [7] authors propose a novel reversible watermarking technique as an improved modification of the existing histogram bin shifting technique. They develop an optimal selection scheme for the "embedding point" (grayscale value of the pixels hosting the watermark), and take advantage of multiple zero frequency pixel values (if available) in the given image to embed the watermark.

II. REVERSIBLE WATERMARKING AND PERCEPTUAL HASHING

A. Revesible Watermarking

Reversible watermarking, also called lossless watermarking, which allows full abstraction of the embedded data along the whole restoration of the cover (image). It can be well-thought-out as a superior case of watermarking. This watermarking technique is ahead more courtesy for the now a days because of its growing applications in many field such as healthcare, military communication, and law-enforcement. Figure 1 shows the basic block diagram of reversible watermarking techniques.

Like a regular watermark, a reversible watermark should have the properties of fidelity, which is measured with PSNR, efficiency, which is evaluated by PSNR vs. bits of information per pixel, and security, which is characterized by how easy it is to extract the embedded information. Furthermore, most reversible watermarks are fragile watermarks: the watermark will be destroyed if there are any changes to the watermarked file. Since the goal of a reversible watermark is so that the original file can be recovered without losses, reversible watermarks do not have to exhibit the robustness property that some watermarks have. In applications that robustness is essential, reversible watermarks can be used in conjunction with a robust watermark.

B. Classification Techniques of Reversible Watermarking

- **Compression Based Reversible Watermarking**
  In order to obtain the original image, we need to accumulate the information essential for recovery of the original image beside with the watermark. Thus, in case of reversible watermarking, extra data needs to be embedded and consequently, requirements more space compared to conventional watermarking for data embedding. A simple approach will be to compress a part of cover image for embedding data.

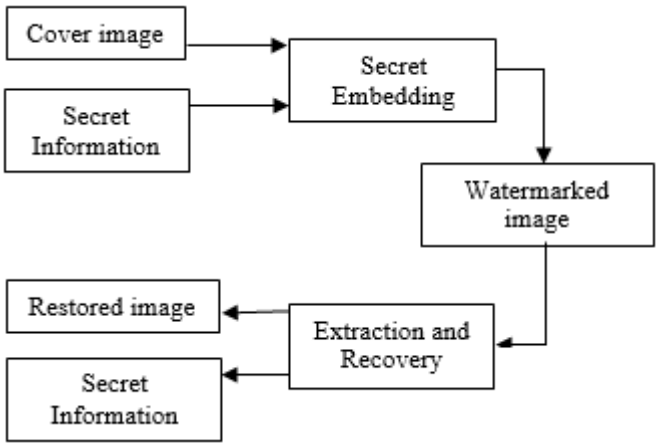

Figure 1: Basic Reversible Watermarking Scheme

- **Histogram modification based reversible watermarking**
  In this, approach, image is divided into several blocks of neighboring pixels. Then, each block is ripped into two zones, and corresponding histograms are calculated. A bin is shifted in accordance with the value of corresponding watermark bit. If the bit is 1, shift the lowest bin to the highest one, and downgrade other bins. And if the bit is 0, then upgrade each bin and shift the highest bin to the lowest bin.
- **Quantization Based Reversible Watermarking**

Quantization based watermarking techniques are, in general, robust. However, the reversible quantization based watermarking approaches are mostly fragile in nature. Cheung et al. (2007) proposed a Sequential Quantization Strategy (SQS) for data embedding. SQS makes the modulation of a pixel value dependent on the previous pixels. A reversible data embedding method is used with SQS to make it more suitable for the authentication purposes. Saberian et al. Presented a Weighted Quantization Method (WQM) approach, which can be functional in spatial as fine as transform domain.

- **Expansion based reversible watermarking**
  Tian (2003) presented a novel approach, named difference expansion (DE). It gave a new direction to the reversible watermarking methods. It achieves high embedding capacity and low computational complexity compared to the preceding techniques.
- **Contrast mapping based reversible watermarking**
  In their technique, they performed transformation of pair of pixels. The alteration is invertible for some pair of pixels, even if LSBs of transformed pairs are lost. The computational rate is low as the method is uncomplicated in nature.
- **Prediction error based reversible watermarking**
  Watermarking scheme based on the association among the neighboring pixels for gray scale images. This correlation is modeled by means of a predictor, which computes the present pixel intensity.
  - **Interpolation based reversible watermarking**
    Image interpolation is a process of estimating the missing pixels. Consider an image of size 2M X 2N, which is down-sampled to get a low resolution (LR) image of size M X N .The pixels present in the low resolution image are called sample pixels. Using these sample pixels, missing pixels of high resolution image i.e., non-sample pixels, are interpolated to construct the interpolated image of size 2M X 2N. The difference between the interpolated pixel value and the original pixel value is called interpolation error.

TABLE 1: COMPARISON OF TECHNIQUES

Technique	Type	Blind/Semi-Blind
Compression based	Fragile	Blind
Histogram based	Semi-Fragile, Robust to JPEG compression	Blind, Semi-Blind
Quantization based	Fragile	Blind
Contrast mapping based	Robust to cropping	Blind
Expansion based	Fragile	Blind

C. Perceptual Hashing

Recently, researchers in the field of security/authentication of multimedia data have introduced a technique inspired from the cryptographic hash functions to authenticate multimedia data called the *Perceptual hash functions* or *Perceptual image hashing* in case of image applications. It should be noted that the objective of a cryptographic hash function and a perceptual image hash function are not exactly the same. For example, there is no robustness or tamper localization requirement in case of a cryptographic hash function (Ahmed & Siyal, 2006) [11].

Traditionally, data integrity issues are addressed by cryptographic hashes or message authentication functions, such as MD5 (Rivest, 1992) and SHA series (NIST, 2008), which are sensitive to every bits of the input message. As a result, the message integrity can be validated when every bit of the message are unchanged (Menezes et al., 1996). This sensitivity to every bit is not suitable for multimedia data, since the information it carries is mostly retained even when the multimedia has undergone various content preserving operations. Therefore, bit-by-bit verification is no longer a suitable method for multimedia data authentication. Robust perceptual image hashing methods have recently been proposed as primitives to overcome the above problems and have constituted the core of a challenging developing research area to academia as well as the multimedia industry. Perceptual Image hashing functions extract certain features from image and calculate a hash value based on these features.

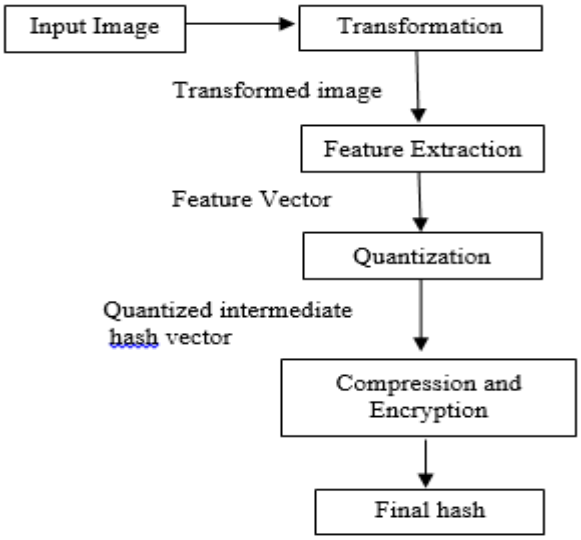

Figure 2: Four Pipelining Stages of perceptual hashing system.

Such functions have been proposed to establish the "perceptual equality" of image content. Image authentication is performed by comparing the hash values of the original image and the image to be authenticated.

Perceptual hashes are expected to be able to survive on acceptable content preserving manipulations and reject malicious manipulations. In recent years, there has been a growing body of research on perceptual image hashing that is increasingly receiving attention in the literature. Perceptual image hashing system generally consists of four pipeline stages: the *Transformation* stage, the *Feature extraction* stage, the *Quantization* stage and the *Compression and Encryption* stage as shown in Fig 2.

The Quantization stage in a perceptual image hashing system is very important to enhance robustness properties and increase randomness to minimize collision probabilities in a perceptual image hashing system. This step is very difficult especially if it is followed by the Compression and Encryption stage because we do not know the behavior of the extracted continuous features after content-preserving/content-changing manipulations. For this reason, in most proposed perceptual image hashing schemes, the Compression and Encryption stage is ignored.

D. Classification of Perceptual Hashing Methods

- **Statistic-based schemes:** This group of schemes extracts hash features by calculating the images statistics in the spatial domain, such as mean, variance, higher moments of image blocks and Histogram.
- **Relation-based schemes:** This category of approaches extracts hash features by making use of some invariant relationships of the coefficients of discrete cosine transform (DCT) or wavelet transform (DWT).
- **Coarse-representation-based schemes:** In this category of methods, the perceptual hashes are calculated by making use of coarse information of the whole image, such as the spatial distribution of significant wavelet coefficients, the low-frequency coefficients of Fourier transform, and so on.
- **Low level feature-based schemes:** The hashes are extracted by detecting the salient image feature points. These methods first perform the DCT or DWT transform on the original image, and then directly make use of the coefficients to generate final hash values. However, these hash values are very sensitive to global as well as local distortions that do not cause perceptually significant changes to the images.

III. LITERATURE SURVEY

TABLE 2. SURVEY TABLE

Sr No	Paper	Robustness	Embedding capacity	Fragile
1.	[3]	N/A	N/A	N/A
2.	[2]	Robust	High	Fragile
3.	[1]	Robust	N/A	N/A
4.	[5]	Robust	High	Fragile
5.	[6]	Robust	Moderate	Fragile
6.	[7]	Robust	High	Fragile
7.	[9]	Robust against JPEG compression	High	Fragile
8.	[13]	N/A	N/A	N/A
9.	[14]	Robust	High	N/A

IV. CONCLUSION

The recent surveyed schemes on reversible watermarking provide the image extraction of low quality and embedding capacity is not high in every image format. The traditional irreversible watermarking schemes will not provide efficient result and reuse of an image is not possible because distortion is too high. The existing work guides a way about the future scope to achieve images which are more reliable and secure image by making some sort of beneficial changes in their work. So by combining both reversible watermarking and perceptual hashing the expected goal may be achieved. The study in this direction may be advantageous to refine essential parameters of image in today's internet world.

REFERENCES

[1] Analysis of Perceptual Hashing System for Secure and Robust Image Hashing. Sahana M S, Veena S K. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 02 Issue: 03 p-ISSN: 2395-0072, June-2015.

[2] High capacity reversible image watermarking using error expansion and context-dependent embedding. A. Siddiqa and A. Khan. Electronics letter (Springer), 2015

[3] A survey on reversible watermarking techniques, Applications and attacks. Thilagavathi N, Saravanan D, Kumarakrishnan S, Sakthivel Punniakodi, J. Amudhavel, Prabu U. ACM, 2015

[4] A recent survey of reversible watermarking techniques. Asifullah Khan, Ayesha Siddiqa, Summuyya Munib, Sana Ambreen Malik. http://dx.doi.org/10.1016/j.ins.2014.03.118 0020-0255/_ 2014 Elsevier Inc.

[5] A new approach to reversible watermarking. Toshiki Ito, Ryo Sugimura, Hyunho Kang, Keiichi Iwamura, Kitahiro Kaneda, Isao Echizen. Tenth Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2014.

[6] A Survey of Digital watermarking techniques, Applications and Attacks. Prabhishek Singh, RS Chauhan, International Journal of Engineering and Innovative Technology (IJEIT), March 2013.

[7] A novel reveresible image authentication scheme for digital images. Chun-Chi Lo,Yu-Chen Hu, Elsevier publication,2013.

[8] Improved histogram bin shifting based reversible watermarking. Pasunuri Nagarju, Ruchira Naskar and Rajat Subhra Chakraborty, International conference on intelligent systems and signal processing (ISSP), 2013.

[9] Robust Image Content Authentication Using Perceptual Hashing and Watermarking. Li Weng, Rony Darazi, Bart Preneel, Benoˆıt Macq, and Ann Dooms,Springer, 2012.

[10] An integrity verification system for images using Hashing and Watermarking. Subheesh Vasu, Sudhish N Gorge, Deepthi P .P. International Conference on Communication Systems and Network Technologies, IEEE, 2012.

[11] A Secure Perceptual Hash Algorithm for Image Content Authentication. Li Weng and Bart Preneel, Springer,2011.

[12] Perceptual Image Hashing. Azhar Hadmi, William Puech, Brahim Ait Es Said and Abdellah Ait Ouahman, 2010.

[13] Reversible image hiding scheme using predictive coding and histogram shifting. Piyu Tsai, Yu-Chen Hu, Hsiu-Lien Yeh. Doi:10.1016/j.sigpro.2008.12.017.

[14] Thesis on Methodologies in Digital watermarking: Robust and Reversible watermarking techniques for Authentication, Security and Privacy Protection. Xin Cindy Guo, 2008.

[15] Reversible Watermarking: Current status and key issues. Jen-Bang Feng, Iuon-Chang Lin, Chwei-Shyong Tsai, Yen-Ping Chu. International Journal of Network Security, Vol.2, No.3, PP.161-171, May2006.

[16] A Secure Perceptual Hash Algorithm for Image Content Authentication. Li Weng and Bart Preneel, Springer,2005.

[17] Reversible watermarking using a perceptual model. Mohammad Awrangjeb Mohan S. Kankanhalli, Journal of Electronic imaging, 2005

[18] Digital image processing third edition, Rafael C. Gonzalez, Richard E. Woods, Pearson publication edition 2012.

[19] Perceptual hashing, http://www.interchopen.com