An Extensive Review on Digital Image Watermarking

Prashant Yadav
Student, Department of Electronics & Communication Engineering
NRI Institute of Research & Technology, Bhopal (M.P.)

Rajesh Kumar Rai
Professor, Department of Electronics & Communication Engineering
NRI Institute of Research & Technology, Bhopal (M.P.)

ABSTRACT
In the past decade, application of digital multimedia contents has grown rapidly because of their advantages over analog contents. Ease of transferring and broadcasting over networks, higher quality and durability, online/offline easy editing, copying, and simplicity of archiving or storing are just a few advantages of digital multimedia over analog contents. Ironically, all the above advantageous properties have raised the main concerns in copyright management and privacy protection of such contents. Encryption methods such as conventional connection-based security systems cannot carry out the required proper protection level as it is impossible to monitor how a legitimate user handles the content after decryption, which makes it possible for hackers and adversaries to illegally redistribute or manipulate the content.

Keywords:
Digital Watermarking, k-means clustering, and Masking.

1. INTRODUCTION
Information hiding, Watermarking, and steganography are three closely related areas which have a lot of common characteristics and share many technical approaches. Information hiding, also known as data hiding, is a general term containing a broad range of problems beyond embedding messages in content. The term hiding can refer to either making the information imperceptible or keeping the very existence of the information secret, as in watermarking and steganography respectively. Steganography is the art of concealed communication where the existence of the message is secret, simple example of such a method is invisible ink. On the other hand, in watermarking the embedded message is directly related to the cover work or host signal. Using these definitions, information hiding systems can be divided into four categories [3]:

1. Covert watermarking: the message is related to the cover work and the existence is hidden.

2. Overt watermarking: the message is related to the cover work and its existence is known.

3. Steganography (covert communication): the message is independent of the cover work and the existence is hidden.

4. Overt embedded communications: the message is unrelated to the cover work and its existence is known.

Watermarking as it is used today may refer to all four categories mentioned above. To address the intended applications properly, in this watermarking refers to the overt watermarking and steganography categories. Furthermore, the still images as a part of the multimedia contents; all the reviews, discussions, and the proposed reversible watermarking scheme and biometric watermark framework principally target digital still images. Although, the suggested algorithms can be modified and adjusted to extend to the video contents. Digital watermarking and Steganography are methods engaged to address such problems. Watermarking is defined as the practice of imperceptibly altering a work to embed a message about that work. On the other hand, steganography is the practice of undetectably altering a work to embed a secret message [3]. These alterations are called as the mark or watermark, which carry informative data for authentication, identification, privacy protection and controlled access purposes. Even though the aims of watermarking and steganography are quite different, both applications share certain high-level elements. Both systems consist of an embedder and a detector, as shown in Fig 1. The embedder takes three inputs, the to-be-embedded payload (watermark), the cover work and the secret key for the protection of the payload. Embedder's output is typically transmitted or recorded. At the detector side, the marked work is presented as an input to the detector. Most detectors try to determine whether a payload is present, and if so, extract the detected payload using the secret key. Studies in this field have been mainly focused on marking methods for still images, digital audio and video contents.

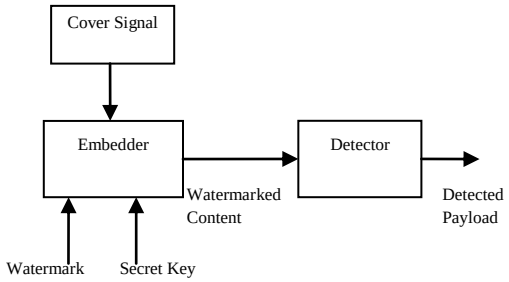

Fig.1 Block diagram of a generic watermarking system.

2. SYSTEM MODEL
Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object. The watermark can be a logo picture, sometimes a binary picture [18], sometimes a ternary picture [19]; it can be a bit stream [16] or also an encrypted bit stream etc. The encryption may be in the form of a hash function [21] or encryption using a secret key [20, 22]. The watermark generation process varies with the owner.

2.1 Encoding Process

In the encoding process both the original data and the payload data are passed through the encoding function. The payload signal and the original host signal now together occupy space, which was previously occupied only by the host signal. For this purpose either the original data is compressed [1, 3, 4, 5 6] or redundancy in digital content is explored to make space for the payload [2].

2.2 Watermark Extraction

Extraction is achieved in two steps. First the watermark or payload is extracted in the decoding process and then the authenticity is established in the comparing process.

2.3 Decoding Process

The decoding process can be itself performed in two different ways. In one process the presence of the original un-watermarked data is required and other where blind decoding is possible. Fig.1.2 and Fig.1.3 show the two processes. A decoder function takes the test data (the test data can be a watermarked or un-watermarked and possibly corrupted) whose ownership is to be determined and recovers the payload.

3. REVERSIBLE WATERMARKING APPROACH

In reversible watermarking, a watermark is embedded in a digital image *I*. This results in a watermarked image *I'*. This image might or might not have been tampered by some intentional or unintentional attack. The watermark can be removed from *I'* to restore the original image, which results in a new image I" ([provided no tampering is taken place). By definition of Reversible watermark the restored image I" will be exactly same as the original image I, pixel-by-pixel, bit-by-bit. Fig. 2 shows Reversible Watermarking Scheme.

The reversible watermark is distortion–free embedding. One essential requirement of digital watermarking is its imperceptibility, embedding a watermark inevitably changes the original content. Even a extremely slight change in pixel values may not be desirable in sensitive imagery, such as military data, medical data and data used in crime detection. In such state, each bit of information is important. Any change will affect the intelligence of the digital content, and the access to the original, raw data is always required. Reversible watermarks will provide the original, raw data for digital content authentication. A basic approach of reversible watermarking algorithms is to select an embedding area in an image, and embed both the payload and the original values in this area.

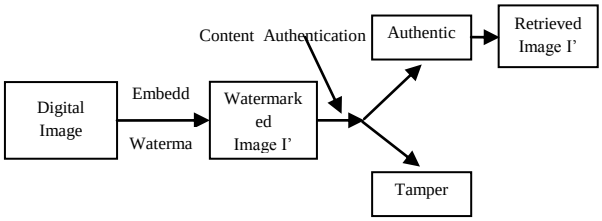

Fig. 2 Reversible Watermarking Scheme

4. LITERATURE REVIEW

Lingling An, Xinbo Gao and Xuelong Li investigated the robust reversible watermarking (RRW) methods are popular in multimedia for protecting copyright, while preserving intactness of host images and providing robustness against unintentional attacks. Hoauthorsver, conventional RRW methods are not readily applicable in practice. That is mainly because: 1) they fail to offer satisfactory reversibility on large-scale image datasets; 2) they have limited robustness in extracting watermarks from the watermarked images destroyed by different unintentional attacks; and 3) some of them suffer from extremely poor invisibility for watermarked images. Therefore, it is necessary to have a framework to address these three problems, and further improve its performance. This research work presents a novel pragmatic framework, wavelet-domain statistical quantity histogram shifting and clustering (WSQH-SC). Compared with conventional methods, WSQH-SC ingeniously constructs new watermark embedding and extraction procedures by histogram shifting and clustering, which are important for improving robustness and reducing run-time complexity. Additionally, WSQH-SC includes the property-inspired pixel adjustment to effectively handle overflow and underflow of pixels. These outcomes in satisfactory reversibility and invisibility. To increase its practical applicability, WSQH-SC designs an enhanced pixel-wise masking to balance robustness and invisibility. Authors perform extensive experiments over natural, medical, and synthetic aperture radar images to show the effectiveness of WSQH-SC by comparing with the histogram rotation-based and histogram distribution constrained methods.

Kavipriya, R. and Maheswari, S. proposed as a solution to the problem of resolving copyright ownership of multimedia data (image, audio and video). Devising effective watermarking schemes especially the security oriented applications like copyright protection, copy control, etc., is an extremely challenging task. Most of the existing reversible watermarking methodologies have much difficulty in practical applicability due to lack of sufficient reversibility in large scale image datasets, poor invisibility and in some cases robustness is destroyed by unintentional attacks. All this have to be addressed in an efficient methodology. The work presented in this research work is concerned with the design of robust digital image watermarking algorithms for copyright protection. In the embedding part, haar wavelet transform is applied to the cover and the watermark image in which the loauthorsr subband coefficients of cover image are statistically analyzed for selection of watermark embedding. To embed the watermark bits, the watermark strength is adjusted using enhanced pixel-wise masking. In the extraction part, an efficient inverse detection algorithm is used for extracting the watermark image. It is experimentally confirmed that this methodology gives excellent outcomes under tested image processing attacks and JPEG compression.Rongrong Ni, Cheng, H.D. and Yao Zhao focused in this research, an error-free authentication watermarking is proposed based on prediction-error-expansion reversible methodology. A binary image is used as an authentication watermark, and embedded in the prediction errors block-wise. A location map is designed and encoded to promise accurate extraction and recovery. A retesting strategy utilizing the parity detection activates the capacity of the ambiguous pixels. In the authentication and recovery period, a watermarked image can be identified as authentic or tampered. If an image is authentic, it can be recovered without errors. The embedded

information can be extracted correctly. If an image is a tampered one, the tampered positions can be labeled. The experimental results show the effectiveness and reliability of the proposed method.Hyobin Lee, Seongwan Kim and Jaeho Lee presented a novel reversible data hiding algorithm, which can recover the original image if it is deemed authentic or detect the block-wise malicious manipulation if it is classified as manipulated. Authors explore the strong spatial correlation of neighboring pixels in digital images to achieve very high embedding capacity and keep the distortion low. Also, this methodology provides cryptographic strength when verifying image integrity because the probability of making undetectable modifications to the image is directly related to a secure cryptographic element, such as a hash function. The algorithm has been successfully applied to a wide range of images, including commonly used images, biometric images, texture images, and aerial images. Experimental outcomes and performance comparison with other reversible data hiding schemes are presented to demonstrate the validity of the proposed algorithm.

Zhiguo Chang, Jian Xu and Authorsidong Kou estimated the fact that the differences betauthorsen the pixel values in the local region of an image are small and propose two simple and effective reversible watermarking schemes based on the spatial quad-based difference expansion that applies the difference expansion to the image in row-wise and column-wise simultaneously. The schemes make good use of both row-wise and column-wise pixel pairs with small differences. Experimental results show our schemes are effective.

Haifeng Zhu; Chunhui Zhao and Chunming Tang researched content-based watermarking scheme for tamper detection and recovery of image is presented. In the scheme, an image is divided into four quadrants firstly. Then correlation groups are set up after some blocks (each size is 8times8) in different two quadrants being matched. Correlative matrix can be got after the blocks of each group correlation operation being processed. This kind of operation is reversible. The watermark which is embedded into the LSB of each block A includes the signature of the block B and a part of correlative matrix of the two blocks B. The block A and block B should be in relatively long distance in image. The advantage of the scheme is that the tamper content is recovered by untampered content. The experimental results show that our scheme can be applied in detecting and localizing any tampering of equal or more than the size of 8times8 pixels.

Bausys, R. and Kriukovas, A. worked on a specific media (military or medical imagery) modifications introduced by watermarking process are not acceptable. Reversible watermarking, that allows to restore exact original image, is designed for this usage. In this research work semi-blind reversible pixel-wise image authentication framework is proposed. The scheme allows us to authenticate and locate tampered pixels. Also exact recovery of the original image is possible.

Puhan, N.B. and Ho, A.T.S. proposed an innovative perception based watermarking algorithm in binary document images for secure authentication purpose. Binary image watermarking with pixel flipping approach is a challenging problem, because flipping the black and white pixels in such simple images can bring noticeable visual distortion. A novel perceptual based model was proposed towards digital watermarking of binary images in the research work of A.T.S. Ho et al. (May 2004). The model estimates the distortion out coming from flipping of a pixel by finding the curvature-author sighted distance difference (CWDD) measure betauthorsen original and watermarked contour segments. In this research work, the reversible property of the CWDD measure is used towards designing a new authentication watermarking algorithm so that the possibility of any undetected modification to the watermarked image is removed. This algorithm embeds an authentication signature computed from the original image into itself after identifying an ordered set of low-distortion pixels. The same ordered set of pixels are correctly found in both the embedder and blind detector through the design of necessary conditions. The ability of the proposed authentication algorithm to detect any modification in the watermarked image is equivalent to the security of cryptographic authentication. The parity attack found in the previous block-wise data hiding methods in binary images is not possible in the proposed algorithm due to pixel-wise embedding of the authentication signature. Simulation results show the imperceptibility of the watermarking process and successful detection of content modifications.

5. PROBLEM DESCRIPTION

The Problem Description is the principal that used to protect the rights of the content owners and probably the most widespread developed scientific method of protecting digital multimedia content. As already explained, encryption maynot help the content owners or the distributors monitor how the content is handled after decryption which may lead to illegal copying and distribution or misuse of the private information. As a result, it is not an overstatement to say that cryptography can protect content in transit, but once decrypted, the content has no further protection. Therefore, there is a strong need for an alternative or compliment technology to cryptography which can protect the content even after it is decrypted. Watermarking technology seems to have the potential of fulfilling such a need as it embeds imperceptible information into the content which is never removed during normal usage or causes inconvenience to the users. A watermark can be designed to survive different processes such as decryption, re-encryption and compression. There are a number of other applications for which watermarking methods may be developed, used, or suggested, although major driving forces behind the watermarking technology have been copyright protection and copy prevention.

6. CONCLUSION

In this review paper we have studied and analyzed the significance of water marking. Watermarking scheme targets a wide range of issues. The requisites of a particular scheme are determined by its application. For establishing ownership, or determining authenticity, the watermarking scheme should satisfy certain issues these are Unobtrusiveness: the watermark should be imperceptible i.e. the watermarked image should be perceptually equal to the original image. The watermark should not degrade or affect the image quality, Robust: the watermark should be resistant to attacks both intentional and unintentional Specifically the various type attacks and a Large data capacity in this the data hiding capacity should be large so that more secret information can be embedded in the image. Future Scope of the idea of this paper is Owner identification, Copy protection , Content authentication ,Fingerprinting, Broadcast monitoring ,Medical applications.

7. REFERENCE

[1] Lingling An , Xinbo Gao,Xuelong Li; Dacheng Tao; Cheng Deng; Jie Li 2012.Robust Reversible Watermarking via Clustering and Enhanced Pixel-Wise Masking.

[2] Kavipriya, R.Maheswari, S.2014 Statistical quantity based reversible watermarking for copyright protection of digital images.

[3] Rongrong Ni, Cheng, H.D. Yao Zhao, Yu Hou. 2013.Error-free authentication watermarking based on prediction-error-expansion reversible methodology.

[4] Hyobin Lee, Seongwan Kim, Jaeho Lee, Sooyeon Kim Sangyoun Lee .2008. Reversible watermarking with localization for biometric images,Control, Automation, Robotics and Vision.

[5] Zhiguo Chang; Jian Xu, Authorsidong Kou,2008. Reversible Watermarking Schemes Using Spatial Quad-Based Difference Expansion.

[6] Haifeng Zhu, Chunhui Zhao, Chunming Tang 2006. A Fragile Watermarking Scheme For Tamper Detection and Recovery of Image.

[7] Bausys, R., Kriukovas, A.2006. Reversible watermarking scheme for image authentication in frequency domain

[8] Puhan, N.B. Ho, A.T.S.,2005. Binary document image watermarking for secure authentication using perceptual modeling.

[9] L. An, X. Gao, C. Deng, and F. Ji,2010. Robust lossless data hiding:

[10] C. De Vleeschouwer, J. Delaigle, and B. Macq, 2001.Circular interpretation of histogram for reversible watermarking.

[11] C. De Vleeschouwer, J. Delaigle, and B. Macq, 2003.Circular interpretation of bijective transformations in lossless watermarking for media asset management.

[12] Z. Ni, Y. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, 2008.Robust lossless image data hiding designed for semi-fragile image authentication

[13] D. Zou, Y. Shi, Z. Ni, and W. Su, 2006.A semi-fragile lossless digital watermarking scheme based on integer wavelet transform.

[14] X. Gao, L. An, Y. Yuan, D. Tao, and X. Li,2011. Lossless data embedding using generalized statistical quantity histogram.

[15] N. Dalal and B. Triggs,2005.Histograms of oriented gradients for human detection.