Reversible De-Identification for Lossless Image Compression using Reversible Watermarking

Kiran Kadam
Department of Information Technology
Siddhant College of Engineering, Sudumbare
Pune, India
E-mail:Kiranarunkadam@gmail.com

Prof. Sonali Rangadale
Department of Information Technology
Siddhant College of Engineering, Sudumbare
Pune, India
E-mail: Sonali_rangdale@rediffmail.com

***Abstract*—Video surveillance cameras are becoming everywhere in many developed countries. This has raised several privacy related issues which have pushed policy makers to regulate their use. One approach to provide safety and privacy is to obfuscate sensitive area within an image/video which prevents the identification of the persons being captured. This method an irreversible obfuscation method which however, prevents the use of the captured videos from aiding criminal investigation or to be used as evidence in court or equivalent area.**

Keywords- obfuscate, reversible watermarking .

I. INTRODUCTION

Image has become hot topic in many research fields. Long Years back images are only used for recording memories, but now images have changed their face. Images may be two-dimensional, like photograph, and can be three-dimensional. They may be captured by optical cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects such as the human eye or water surfaces. Today, images can be used for encryption, processing, authentication, storage, sharing etc. purpose. But the main aim of image is still being preserved i.e. to store and maintain the memories. Sometimes useful images get misused when shared over social networking sites.

Digital watermarking techniques have been identified so far as a possible solution when, in a specific application scenario (authentication, security, copyright protection etc), there is the need to embed an informative and encrypted message in a digital document in an imperceptible way. Such a goal is basically achieved by performing a slight modification/addition to the original data trying to, at the same time; satisfy other bindings such as capacity, reliability and robustness. What is important to highlight, beyond the way all these issues are achieved, it is that this "slight modification" is irreversible and timely available: the watermarked content is different from the original one. This means that any successive assertion, usage, and evaluation must happen on a, though weakly, corrupted version, if original data have not been stored and are not readily available. It is now clear that in dependence of the application scenario, this cannot always be acceptable. Usually when dealing with sensitive imagery such as deep space science, military operations, and researches, and medical diagnosis, the end-user cannot tolerate to risk getting distorted information from what he is watching at. One example above all: a radiologist who is checking a radiographic image to establish if a certain pathology is present or not.

Reversible watermarking techniques are also named as invertible or lossless and were born to be applied mainly in scenarios where the authenticity and security of a digital image has to be granted and the original content is peremptorily needed at the decoding side. Here it's important to point out that, initially, a high quality of the watermarked image was not a requirement due to the fact that the original one was recoverable and simple problems of overflow and underflow caused by the watermarking process were not taken into account too. Successively also, this aspect has been considered as basic to permit to the end user to operate on the watermarked image and to possibly decide to resort to the uncorrupted version in a second time if needed.

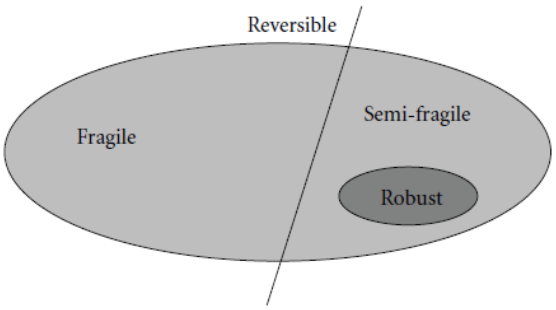

Fig. 1Watermarking Types

The exemplar based SR, correspondences between HR and LR patches are learned from a group of HR-LR patches known as Dictionary and then applied to a low resolution image to recover its higher resolution version. SR methods consider Super Resolution image reconstruction as a deblurring problem and solve the inverse problem using Bregman iterations. The HR image is estimated based on some prior knowledge about the image in the form of regularization. A new regularization method based on multi scale morphological filters is proposed.

II. LITERATURE SURVEY

This section shows existing water margining technique and their work. The emerging research area of Digital

watermarking is combination of concepts derived from computer science, cryptography, signal and image processing and communications[1]. Reversible watermarking has found a huge surge of experimentation in its domain in recent era as the need of recovering the original work image after extracting the watermark arises in various applications such as the law enforcement, medical and military image system, it is important to restore the original image without any distortions. The main purpose of digital watermarking is to embed little amount of secret information, i.e., the watermark into the host digital productions similar to the image and audio, thereby assisting the extraction at a recovering stage for a range of functions including copyright assertion, authentication, and content integrity verification and many more[4]. In traditional watermarking techniques, our main concern is to embed and recover the watermark with min loss. The quality of original work image we get after extraction is highly degraded and not restorable. But in applications like law enforcement, medical and military, in which better quality of image is needed, we cannot use these algorithms. In medical images, some prerequisite information about the patient is watermarked in it while transmitting and at reception we need to have both, the original image and that information to be recovered lossless[4]. Watermarking methodologies have drawn highly attention due to the remarkable results they produced. It is possible to utilize the Digital watermarking techniques for the protection of the cerebral rights of the data through the embedding of the proprietary information like a password or the company's logo, in the host data[5]. The two significant purposes of a watermark include identification of ownership and the detection of tampering.

The reversible watermark technique we proposed uses the difference of H virtual border to embed an image signature[4]. Virtual border is a mirror of image border line. Authentication is done by comparing the extracting data from virtual border with the hashing of original image. This original image can be restored by the eliminating of virtual border and added watermark. Because of this reversibility, it can be used to watermark a sensitive image that cannot allow a change, although it is a small change[6]. The original images used in this paper are in the RGB color format and in the "png" file format. Majorities are medical images. The size of watermarked image will be increased 2 point in height. It is caused by adding virtual border as embedding media. Image cross is gained from hashing image using standard hash function.

III. PROPOSED SYSTEM

Here we are going to apply several numbers of techniques on input image. Finally the combination of all the result is generalized to produce output. Then the output produced is pass under separate super resolution method.

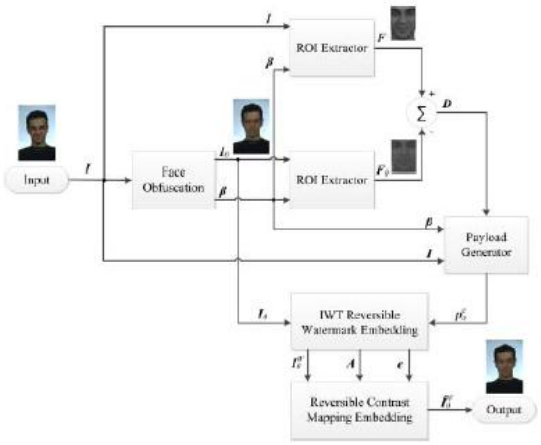

Fig. 2 Encryption method

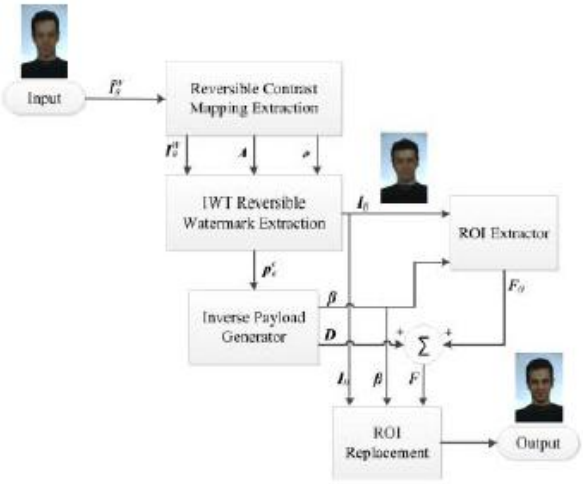

Fig. 3 Decryption method

in spite of the fact that watermarking is engaged in numerous applications, the threat to security for the embedded watermark against probable malicious attacks is not yet been completely feint out. Digital watermarking embeds a certain quantity of information in associated with the ownership into the digital data, thereby assuring copyright protection. Proposed for variety of purposes including copyright protection, access control, and broadcast monitoring, the extraction of the embedded data in the future seems probable. The information regarding ownership can be any privacy information that completely recognizes the owner when ownership controversies arise, such as password, logo or the like. There is a possibility for the abovementioned information being hacked. In addition, there were also chances for the owner to lose or forget the same. The hackers might strength the information occasionally and assert ownership towards the end. The issue of rightful ownership has not yet been appropriately resolved. Thus it is essential that the design of DRM system addresses the abovementioned security issues besides solving the ownership dispute. In this paper, our earlier work has been improved with an effective approach for the generation of watermark data. Avoidance of disputes that arise out of ownership claims on digital

images is our major focus and a capable scheme is proposed to deal with it. In order to guard the digital contents we use watermarking as well as biometrics. The principal purpose of utilizing biometrics is mainly because of its few characteristics such as security and confidentiality. Biometrics is a speedily developing technology which is widely applicable in forensics like the criminal identification and prison security and possibly used by a wide variety of application areas. Henceforth, an imperative role will be occupied by biometrics in security. At last by inserting the biometric feature known as 'watermark' helps to solve if there is any ownership dispute. The minutiae points are taken out from the fingerprint of the owner in the developed scheme. Then the coordinates i.e., the location of the minutiae points are determined and shuffled on the basis of the approach discussed. Subsequently, a vector is formed from the shuffled coordinates of minutiae points. The singular values of this vector is then calculated and used as the watermark.

IV. ALGORITHM OVERVIEW

Single Image resolution algorithm is used reconstruct high resolution images. Here patch of higher resolution from sample database of stored patches is picked and user for watermarking. The main steps are as below

First image will accpepted from user and then forward de-identification proccess will be implied on image along with predefined secure key. Watermarked image will be stored on some location. In Reversible step that image will be passed thorough reverse de-identification phase along with secure and ROI. Image will be recovred based on the ROI and predefined key and reversible watermark.

Reversible watermark is a major subset if fragile watermark. Like all fragile watermarks, It can be used for digital content verification. But reversible watermark is much more than content endorsement. It has an additional advantage that when watermarked content has been detected to be authentic, one can remove the watermark to retrieve the original, un-watermarked content

V. EXPERIMENTAL RESULTS

Two versions of proposed method are defined based on parameters. One uses down sampling factor of 4 in having patch size 5x5 and other is set to 2 having patch size 7x7.

Uncompressed data such as audio graphics and video require considerable high storage capacity and transmission bandwidth than usual. in spite of rapid growth in mass storage density and significant improvement in communication channel bandwidth, demand for data storage capacity and transmission bandwidth continues to outshine the capabilities of existing technologies. One approach to mitigate this problem is to reduce the size of multimedia data transmitted over the communication channel via data compression techniques such as JPEG, JPEQ-2000 (Jena et al.). These approaches concentrate on achieving higher compression ratio without sacrificing the quality of the original image. The Image data compression technique, concerned with the reduction of number of bits required to store and transmit image without appreciable loss of information. A fundamental shift in the image compression approach came after the Discrete Wavelet Transform became popular. To overcome the inefficiencies in the JPEG standard and serve emerging areas of mobile multimedia and internet communication, recently the JPEG committee has released its new image coding standard, JPEG-2000, which has been based upon DWT. The Discrete wavelet transform has gained widespread acceptance in signal processing and image compression. Because of their natural multi-resolution nature, wavelet-coding schemes are especially suitable for applications where scalability and tolerable degradation are important.

VI. CONCLUSION

In this paper we have surveyed the current literatures on reversible watermarking which is a recent hot topic of many research areas. We have also classified reversible watermarking algorithms. Due to the space limitations we are not able to put enough technical details here but we have tried to be as much as possible. We have discussed all the above techniques based on PSNR and Embedding Capacity. If we increase the embedding capacity the PSNR gets reduced and vice versa. So we have to maintain an optimum balance between them to get a satisfactory result. A good and reliable technique should have PSNR as well as high Embedding Capacity. Handling of geometric distortion remains a difficult task. More robust system will have significantly leaded the area like Secure reversible watermarking with any attack.

ACKNOWLEDGMENT

Author would like to take this opportunity to express our profound gratitude and deep regard to my Project Guide for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the

project. His valuable suggestions were of immense help throughout my project work. His perceptive criticism kept me working to make this project in a much better way. Working under him was an extremely knowledgeable experience for me.

REFERENCES

[1] Combination of Encryption and Digital Watermarking Techniques used for Security and Copyright Protection of Still Image - IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur India

[2] JPEG Anti-Forensics With Improved Tradeoff Between Forensic Undetectability and Image Quality- IEEE transactions on information forensics and security, vol. 9, no. 8, august 2014

[3] Reversible De-Identification for Lossless Image Compression using Reversible Watermarking - MIPRO 2014, 26-30 May 2014, Opatija, Croatia

[4] ReversibleWatermarking Using Difference of Virtual Border for Digital Image Protection - 2010 International Conference on Distributed Frameworks for Multimedia Applications (DFmA)

[5] Digital image watermarking by using discrete wavelet Transform and discrete cosine transform and Comparison based on psnr - 978-0-7695-4437-3/11 26.00 Â© 2011 IEEE

[6] A lossless color image compression method based on a new reversible color transforms - INMC, Dept. of Electrical Engineering and Computer Science Seoul National University, Seoul 151-744 Korea

[7] Reversible Image Watermarking Using Integer Transform on Lifting Wavelet Coeficients - Chi-Man Pun, Noppom Hemman and Xiao-Chen Yuan [8] An eficient copyright protection scheme for digital images using Biometrics and Watermarking - 978-1-4244-4520-2/09/25.00 Â©2009 IEEE

[8] Reversible Wavelet and Spectral Transforms for Lossless Compression of Color Images - 0-8186-8821-1/98 10.00 0 1998 IEEE

A Survey of Digital Watermarking Techniques, Applications and Attacks - International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013