International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2585
Volume 4, Issue 5, May-2018

Reversible Watermarking Approach For Compression Image

Korrapatti Mohammed Ghouse[1],R Pavan kumr[2]
[1,2]Faculty in Department of ECE, IIIT RK VALLEY-RGUKT AP,
Kadapa, AP

ABSTRACT - This project deals with the De-Identification for Lossless Image Compression using reversible watermarking process. De-Identification is a process which can be used to ensure privacy by concealing the identity of individuals captured by video surveillance systems. One important challenge is to make the obfuscation process reversible so that the original image/video can be recovered by persons in possession of the right security credentials. This work presents a novel Reversible De-Identification method that can be used in conjunction with any obfuscation process. The residual information needed to reverse the obfuscation process is compressed, authenticated, encrypted and embedded within the obfuscated image using a two-level Reversible Watermarking scheme. The proposed method ensures an overall single-pass embedding capacity of 1.25 bpp, where 99.8% of the images considered required less than 0.8 bpp while none of them required more than 1.1 bpp. Experimental results further demonstrate that the proposed method managed using MATLAB12.1a.

Keywords: Watermarking, De-Identification process, obfuscation process, Wavelet Transform.

1. INTRODUCTION

Reversible data hiding (RDH) aims to embed secret message into a cover image by slightly modifying its pixel values, and, unlike conventional data hiding, the embedded message as well as the cover image should be completely recovered from the marked content. RDH is a special type of information hiding and its feasibility is mainly due to the lossless compressibility of natural images. The reversibility in RDH is quite desirable and helpful in some practical applications such as medical image processing, multimedia archive management, image trans-coding, and video error-concealment coding, etc. Generally, the performance of a RDH scheme is evaluated by the capacity-distortion behavior. For a required embedding capacity (EC), to obtain a good marked image quality, one expects to reduce the embedding distortion as much as possible.

Many RDH methods have been proposed so far, e.g., the methods based on lossless compression, difference expansion, histogram modification], prediction-error expansion, and integer transform, etc. Among them, the histogram-based ones have attracted much attention. The histogram-based methods modify the histogram in such a way that certain bins are shifted to create vacant space while some other bins are utilized to carry data by filling the vacant space. This type of methods can well control the embedding distortion and provide a sufficient EC.

The first histogram-based RDH method is the one proposed. This method uses peak and minimum points of the pixel-intensity-histogram to embed data. It changes each pixel value at most by 1, and thus a good marked image quality can be obtained. However, its EC is quite low and this method does not work well if the cover image has a flat histogram. To facilitate it, proposed to utilize the difference-histogram instead. This novel method exploits the correlation among neighboring pixels and can embed larger payload with reduced distortion compared with Ni et al.'s. Moreover, we will see later (see Section III-A) that Lee et al.'s method can be in fact implemented, in an equivalent way, by modifying the two-dimensional pixel-intensity-histogram according to a pixel-pair-mapping (PPM) which is an injective mapping defined on pixel-pairs. In this light, the superiority of Lee et al.'s method over it is explained in another viewpoint. Afterwards, Fallahpour introduced a method by modifying the histogram of prediction-error. Like difference-histogram, the prediction-error-histogram is also Laplacian-like and sharply distributed which guarantees an excellent embedding performance. Instead of only using the correlation of two adjacent pixels in Lee et al.'s method, Fallahpour's method can exploit the local correlation of a larger neighborhood, and thus can provide relatively better performance. Besides the aforementioned methods, many other works are also based on histogram by incorporating some strategies such as double-layered embedding, embedding-position-selection, adaptive embedding, context-modification, and optimal-bins-selection, etc**...** We remark that, the histogram-based RDH methods generally contain two basic steps

Histogram Generation

First, each local image region consisting of several pixels (e.g., a pixel-pair consisting of two adjacent pixels) is projected to a one-dimensional space (e.g., difference value of a pixel-pair) to get a scalar sequence. Then, a one-dimensional histogram (e.g., difference- histogram) is generated by counting the frequency of the resulting sequence.

Histogram Modification

Finally, embed data into the cover image by modifying the histogram. In most cases, the histogram bins with high frequencies are expanded to carry data while some others are shifted to ensure the reversibility.

2. SYSTEM OVERVIEW

In the first step, the complex local image correlation is simplified to a one-dimensional statistic. Clearly, by this simplification, the image redundancy cannot be fully exploited and it only contributes to the second step since a one-dimensional histogram is easy to deal with. Based on this consideration, instead of one-dimensional histogram used in current RDH methods and to better exploit the image redundancy, we propose in this paper a novel RDH scheme by using a two-dimensional difference-histogram.

For the proposed method, by considering a pixel-pair and its context, a local image region is projected to a two-dimensional space to obtain a sequence consisting of difference-pairs. Then, a two-dimensional difference-histogram is generated by counting the difference-pairs. Finally, reversible data embedding is implemented according to a specifically designed difference-pair-mapping (DPM). Here, the DPM is an injective mapping defined on difference-pairs, and it is a natural extension of expansion embedding and shifting techniques used in current histogram-based methods. By using the two-dimensional difference-histogram and this specific DPM, compared with the conventional one-dimensional histogram based methods, more pixels are used for carrying data while the number of shifted pixels is reduced as well, and thus an improved embedding performance is achieved. In addition, inspired by the embedding-position-selection techniques introduced in previous works, a pixel-pair-selection strategy is adopted in our method to priory use the pixel-pairs located in smooth image regions to embed data. This may further enhance the embedding performance. Experimental results demonstrate that the proposed method outperforms some state-of-the-art works.

3. FORWARD REVERSIBLE

DE-DENTIFICATION PROCESS

Fig. 1 illustrates the schematic diagram of the Forward Reversible De-Identification process which receives the original image ***I*** and conceals the face of the person using the ***Face Obfuscation*** process to generate an obfuscated image $\boldsymbol{I}_{\Theta}$. This work considers color images using the YC_bC_r color space. The coordinates of the top left corner and bottom right corner of the De-identified region is enclosed within the bounding box $\boldsymbol{\beta}$, which is passed to both *ROI Extraction* processes to extract the face image ***F*** and the obfuscated face image $\boldsymbol{F}_{\Theta}$. The face images are then subtracted to derive the difference face image ***D.***

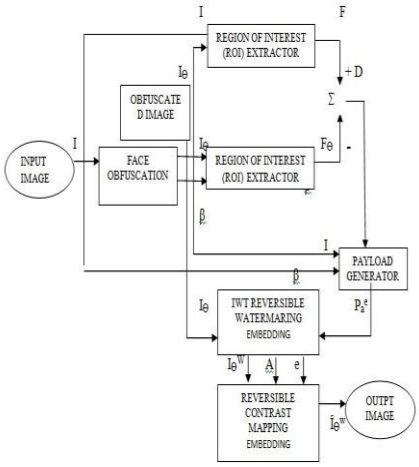


Figure1. Schematic diagram of the Forward Reversible De-Identifcation Process

Face Obfuscation

The *Face Obfuscation* process receives the original image $\boldsymbol{I}$ and detects the face region and eye locations using the ground truth information available in the color FERET dataset. This can be automated using the face detector in [12] and the eye detector in [13] which ensure high accuracies. However, the main contribution of this work is to present a Reversible De-Identification method which is independent from the obfuscation process. Thus, the automation of the face and eye detectors is not in the scope of this work.

The upper left and bottom right coordinates of the face region are included in the bounding box $\boldsymbol{\beta}$ and used to extract the face $\boldsymbol{F}$ which is aligned using affine transformations [14]. The aligned face image $\boldsymbol{F}$ is then concealed using the *k*-same algorithm, which computes the average face derived over the *k* closest aligned faces in Eigen-space, to generate the obfuscated aligned face image $\boldsymbol{F}_{\Theta}$. More information on the *k*-same algorithm can be found in [2]. The obfuscated face image $\boldsymbol{F}_{\Theta}$ is then re-aligned to match the orientation of the original face image $\boldsymbol{F}$ using affine transformations and then overwrites the face region in the original image $\boldsymbol{I}$ to derive the obfuscated image $\boldsymbol{I}_{\Theta}$.

ROI Extraction

The *ROI Extraction* process is a simple algorithm which employs the bounding box coordinates $\boldsymbol{\beta}$ to identify the region to be cropped from the input image $\boldsymbol{I}$ (or $\boldsymbol{I}_{\Theta}$). The cropped sub-image is then stored in the face image $\boldsymbol{F}$ (or obfuscated face image $\boldsymbol{F}_{\Theta}$).

***Payload Generator* Process**

The *Payload Generator* process is then used to convert the difference face image $\boldsymbol{D}$ and bounding box $\boldsymbol{\beta}$ into a packet $\boldsymbol{p}^{e}_{a}$ which is authenticated and encrypted. The packet $\boldsymbol{p}^{e}_{a}$ is then embedded within the obfuscated image $\boldsymbol{I}_{\Theta}$ using the *Integer Wavelet Transform (IWT) Reversible Watermark Embedding* process (1st level) which generates the embedded image $\boldsymbol{I}^{W}_{\theta}$, the auxiliary information $\boldsymbol{A}$ and the residual bit stream $\boldsymbol{e}$. This method provides a good compromise between capacity and distortion. However, additional information might be needed at the receiver to resolve overflow and underflow issues. The *Reversible Contrast Mapping Embedding* process (2nd level) is therefore used to embed this information ($\boldsymbol{A}$ and $\boldsymbol{e}$) within the embedded image $\boldsymbol{I}^{W}_{\theta}$, which usually corresponds to few bits, and generates the second level embedded obfuscated image $\hat{\boldsymbol{I}}^{W}_{\theta}$. This method is ideal since it does not need additional information to resolve overflow/underflow issues. Moreover, the distortions introduced at low bit rates are generally negligible. However, its performance significantly degrades at higher bitrates and is therefore not suitable to embed large payloads.

Fig2. The authenticated packet $\boldsymbol{pa}$

IWT Reversible Watermarking Embedding

The IWT Reversible Watermarking Embedding process first derives the number of decompositions N_{dec} needed to embed the packet p_a^e and C represents the capacity needed to embed p_a^e bits and is computed using

$$C = \frac{\left|\mathbf{p}_a^e\right|}{Ch \times W \times H}$$

where $|\ |$ represents the cardinality of the set, W and H represent the number of columns and rows in the image and Ch represents the number of color channels . This process then adopts the CDF (2,2) integer wavelet transform specified to decompose the image. This method employs Forward Integer Wavelet Expansion to embed the actual information while a novel Threshold Selection strategy is used to identify the set of thresholds which provide enough capacity while minimize the overall distortions. More information is provided in the following subsections.

Reversible Contrast Mapping

The only problem with the proposed *Forward Integer Wavelet Expansion* process is that sometimes $\boldsymbol{A}$ and $\boldsymbol{e}$ are not empty. This work adopts the syntax shown in Fig. 5 to represent this information $\boldsymbol{r}$ to be embedded. The *Flag* is a 2-bit field which indicates whether $\boldsymbol{A}$ and $\boldsymbol{e}$ are empty or not. In case that one of them (or both) are not empty, the number of bits needed to embed the information in $\boldsymbol{A}$ (or $\boldsymbol{e}$) is signaled in N_A (or N_e). The fields N_A and N_e are encoded using 8-bits each while the size of $\boldsymbol{A}$ and $\boldsymbol{e}$ are variable length.

This work adopts the Reversible Contrast Mapping (RCM) to embed the packet $\boldsymbol{r}$ within the watermarked obfuscated image $\boldsymbol{I}^{W}{}_{\theta}$. The main advantage of using RCM is that it embeds all information within the image without any ambiguities and provides an additional capacity of 0.5 bpp. However, the main limitation of the RCM is its limited capacity and that the distortion can become significant when embedding large payloads. However, the packet size $\boldsymbol{r}$ is expected to be very low (generally 2-bits).

	Flag Values	
	A	***e***
Flag	0	0
Flag N_e ***e***	0	1
Flag N_A ***A***	1	0
Flag N_A ***A*** N_e ***e***	1	1

Fig3. The packet *r* to be embedded within $I^{W}\theta$.

The forward RCM transforms two neighboring pixel pairs (x, y) into (x', y') using

$$x' \quad 2x \quad y, y' \quad 2y \quad x$$

To prevent overflow and underflow, the transform is restricted to a sub-domain defined by the pixels which satisfy the conditions

$$0 \quad 2x \; y \quad 255, 0 \quad 2y \; x \quad 255 \quad \forall$$

The RCM scheme replaces the least significant bits (LSBs) of the transformed pairs (x', y'). The LSB of x' is used to indicate whether information is embedded within y' or not. A value of '1' indicates that information is embedded while a value of '0' can indicate two things. It can be that both pixel pair values (x, y) were odd or else that the pair are ambiguous and cannot be used for embedding. In the former case, the information bit is still embedded within the LSB of y'. On the other hand, the latter case cannot be used to embed information and thus the LSB of y' is not changed, while the true value of the LSB of x is inserted within the bit-sequence being embedded.

4. PROPOSED SYSTEM

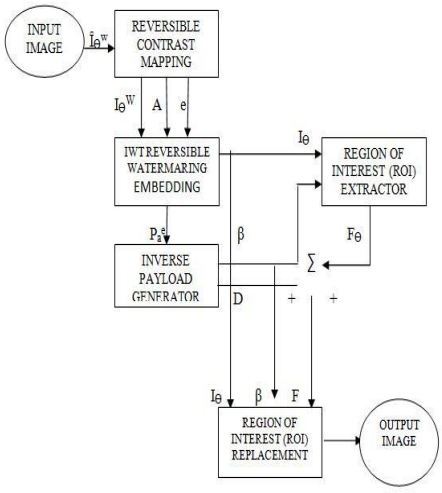


Figure4. Schematic diagram of the Inverse - Reversible De-Identification Process

Fig4. Depicts the schematic diagram of the Inverse Reversible De-Identification process. The second order embedded obfuscated image $\hat{\boldsymbol{I}}^{W}_{\theta}$ is inputted to the *Reversible Contrast Mapping Extraction* process which extracts the first level embedded obfuscated image $\boldsymbol{I}^{W}_{\theta}$ together with the auxiliary information $\boldsymbol{A}$ and the residual bit stream $\boldsymbol{e}$. The *IWT Reversible Watermark Extraction* process is then used to extract the original payload $\boldsymbol{p}^{e}_{a}$ and original obfuscated image $\boldsymbol{I}_{\Theta}$. The *Inverse Payload Generator* reverses the process of the *Payload Generator* and recovers the difference image $\boldsymbol{D}$ and the bounding box $\boldsymbol{\beta}$, which is used by the *ROI Extractor* process to extract the obfuscated face $\boldsymbol{F}_{\Theta}$. The difference image $\boldsymbol{D}$ and obfuscated face $\boldsymbol{F}_{\Theta}$ are then summed to derive the original face $\boldsymbol{F}$, which is used by the *ROI Replacement* process to recover the original image $\boldsymbol{I}_{rec}$.

It is important to notice at this stage that the packet $\boldsymbol{p}^{e}_{a}$ is authenticated and encrypted, and therefore the difference image $\boldsymbol{D}$ and bounding box $\boldsymbol{\beta}$ can only be recovered correctly by persons in possession of the correct security key. The embedding processes are chosen in order to provide minimal distortion so that it maintains the naturalness of the obfuscated image. Moreover, the authentication process ensures that the original image is recovered and ensures that the image is not modified.

Reversible Contrast Mapping Extraction

The *Reversible Contrast Mapping Extraction* process receives the image $\hat{\boldsymbol{I}}_{\theta}^{W}$ and recovers $\boldsymbol{I}_{\theta}^{W}$ and $\boldsymbol{r}$. The information bit can be extracted from the LSB of *y′* when the LSB of *x′* is '1'. However, in the event when the LSB of *x′* is '0', both LSBs of *x′* and y' are forced to be odd and condition (9) is checked. If the condition is satisfied it then represents an odd pixel pair while if it does not it indicates that $y = y'$ and the original LSB value of x is extracted from the bit stream. More information about this is available in . The auxiliary information $\boldsymbol{A}$ and residual bit stream $\boldsymbol{e}$ are then extracted from the packet $\boldsymbol{r}$.

IWT Reversible Watermarking Extraction

The IWT Reversible Watermarking Extraction reverses the IWT Reversible Watermarking Embedding process and extracts the payload information p_a^e and the original obfuscated image I_Θ. It must be noted here that initially, the decoder has no knowledge about the number of decompositions employed N_{dec} and the threshold values T. The decoder thus assumes that a single decomposition is employed and that the threshold values are set to zero. These values are then updated once they are extracted from the header information of s. It is important that the encoder does the same thing during embedding in order to ensure synchronization between the encoder and decoder.

ROI Replacement

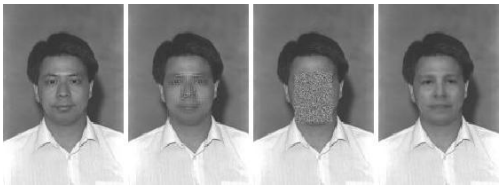
The ROI Replacement process replaces the region marked by the bounding box β with the recovered face image F. The image I_{rec} can be authenticated by comparing the hash derived by computing the SHA-1 on I_{rec} to the Hash value present in the tail of the packet pa.

5. SIMULATION RESULTS

All images considered in this work were converted in the YC_bC_r color space using 4:4:4 sampling. The standard test images were used to evaluate the effectiveness of the proposed Threshold Selection process while the frontal images were used to evaluate the whole system.

The proposed algorithm has set the maximum number of decompositions M to 3 which ensures a single pass embedding capacity offered by the first level of watermarking of 0.9844 bpp. The Difference Expansion method was configured using values suggested and thus adopted $\alpha = 0.5$, NP = 100 and $\Gamma = 0.3$. This paper does not claim that this corresponds to an optimal configuration, but claims that it provides performance superior to state of the art IWT threshold selection schemes .Fig 5 shown below clearly demonstrate that the proposed scheme manages to provide better quality of the stego image I_Θ at different capacities. Simulation results further demonstrate that the proposed scheme needs on average 20 generations to converge. This corresponds to 2000 invocations of the fitness function which is significantly less than the 255NT invocations needed by exhaustive search.

It can be seen that a capacity smaller than 0.8 bpp is needed 99.8% of the time while they never require more than 1.1 bpp. It must be mentioned that the proposed scheme has a single-pass embedding capacity close to 0.307bpp and is thus able to embed the information necessary to recover all images considered in this test. It is important to mention here that frontal images represent a very difficult scenario for our system since the area covered by the ROI is large in relation to the background. Lower capacities are expected when considering common surveillance scenarios. Simulation results further demonstrate that the residual bit stream $\boldsymbol{e}$ was empty for 99.8% of the time and the Auxiliary information $\boldsymbol{A}$ was empty for 99.85% of the time. This result confirms that most of the time the RCM reversible watermarking scheme embeds just 2-bits within the obfuscated image. Moreover, the additional capacity needed in these circumstances was at most 0.015bpp, which is very small and provides negligible distortions.



(a) (b) (c) (d)

Fig 5. Comparing the resulting reversible de-identified images (a) Original Image, (b) Scrambling of DCT coefficients, (c) Encryption of pixel values and (d) proposed method.

6. CONLUSION

This work presents a novel Reversible De-Identification method for lossless compressed images. The proposed scheme is generic and can be employed with other obfuscation strategies other than *k*-Same. A two level Reversible-Watermarking scheme was adopted which uses Differential Evolution to find the optimal set of thresholds and provides a single-pass embedding capacity close to 0.307 bpp. Simulation results have shown that this method is able to recover the original image if the correct encryption key is employed. It further shows that 1.1 bpp were sufficient to cater for 99.8% of the frontal images considered and none of the image needed more than 1.1 bpp. Future work is focused on the extension of color transformations for existing paper the color transformation was yc_bc_r and the extension is lab transformation.

REFFERENCE

[1]. MIPRO 2014, 26-30 May 2014, Opatija, Croatia “Reversible De-Identification for Lossless Image Compression using Reversible Watermarking” ReubenA.Farrugia*Department of Communications and Computer Engineering,University of Malta, Msida, Malta.

[2]. E.M. Newton, L. Sweeney and B. Malin, "Preserving privacy by de-identifying face images," IEEE Trans. on Knowl. and Data Eng., vol. 17, no. 2, pp. 232-243, Feb. 2005.

[3]. W. Zhang, S.S. Cheung and M. Chen, "Hiding privacy information in video surveillance systems," in IEEE Int. Conf. on Image Processing, Genoa, Italy, Sep. 2005.

[4]. I. Martinez-Ponte, X. Desumont, J. Meessen and J.F. Delaigle, "Robust Human Face Hiding ensuring Privacy," in Proc. of Int. Workshop on Image Analysis for Multimedia Services, Montreux, Switzerland, Apr. 2005.

[5]. T.E. Boult, "Pico: Privacy throough invertible cryptographic obscuration," in IEEE Proc. of the Computer Vision for Interactive Intelligent Environment, Whashington DC, USA, Nov. 2005.

[6].A. Senior, S. Pankanti, A. Hampapur, L. Brown,Y. Li Tian and A. Ekin, "Blinkering Surveillance: Enabling video privacy through Computer Vision," *IBM Research Report*, vol. 22886, 2003.

[7]. E.M. Newton, L. Sweeney and B. Malin, "Preserving privacy by de-identifying face images," *IEEE Trans. on Knowl. and Data Eng.*, vol. 17, no. 2, pp. 232-243, Feb. 2005.

[8]. W. Zhang, S.S. Cheung and M. Chen, "Hiding privacy information in video surveillance systems," in *IEEE Int. Conf. on Image Processing*, Genoa, Italy, Sep. 2005.

[9]. I. Martinez-Ponte, X. Desumont, J. Meessen and J.F. Delaigle, "Robust Human Face Hiding ensuring Privacy," in *Proc. of Int. Workshop on Image Analysis for Multimedia Services*, Montreux, Switzerland, Apr. 2005.

[10]. T.E. Boult, "Pico: Privacy throough invertible cryptographic obscuration," in *IEEE Proc. of the Computer Vision for Interactive Intelligent Environment*, Whashington DC, USA, Nov. 2005.

[11]. F. Dufaux, M. Ouaret, Y. Abdeljaoued, A. Navarro, F. Bergnenegre and T. Ebrahimi, "Privacy Enabling Technology for Video Surveillance," in *SPIE Mobile Multimedia/Image Processing for Military and Security Applications*, Orlando, Florida, May 2006.