International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Face Obfuscation Based Reversible Watermarking For Lossless Image Compression

Vivek Jaladi[1], Suhasini Andurey[2]

[1]Assistat Professor, Lingraj Appa Engineering College Bidar-585403

[2]M.Tech Final Year (VLSI Design and Embedded Systems) 2015, Lingraj Appa Engineering College Bidar-585403

Abstract: ***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 to recover and authenticate all images considered. It is also possible to obfuscate the image with video it creates ample opportunities for the sharing of video sequences. In order to protect the privacy of subjects visible in the scene, automated methods to de-identify the images, particularly the face region are necessary.***

Keywords: Obfuscation, Watermarking, Forward Reversible De-Identification, Inverse Reversible De-Identification.

1. Introduction

In today's growing world of technology video surveillance cameras are becoming ubiquitous so the issue of protecting personal information has emerged as a much more important topic. Many studies and social interests have been concentrated on the protection of the images, such as facial images, where privacy protection is required. However, changes in the life environment caused by the rapid development of digital media techniques and communication media have changed users' emotional and sensual feelings. As a result, the study on human senses and sensibility has been carried out in earnest to satisfy user needs through the convergence of many different fields. It is required to develop image obfuscation techniques which can minimize the infringement of user sensibility and simultaneously protect private life. Therefore, it is necessary to develop image distortion techniques to minimize the infringement of user sensibility and protect their privacy. Video cameras are being installed in urban areas throughout the developed world, intended principally as a deterrent to crime. The argument is that crimes will not be committed (or will be committed elsewhere) because of the likelihood of being caught in the act by active surveillance, or identified later from video recordings.

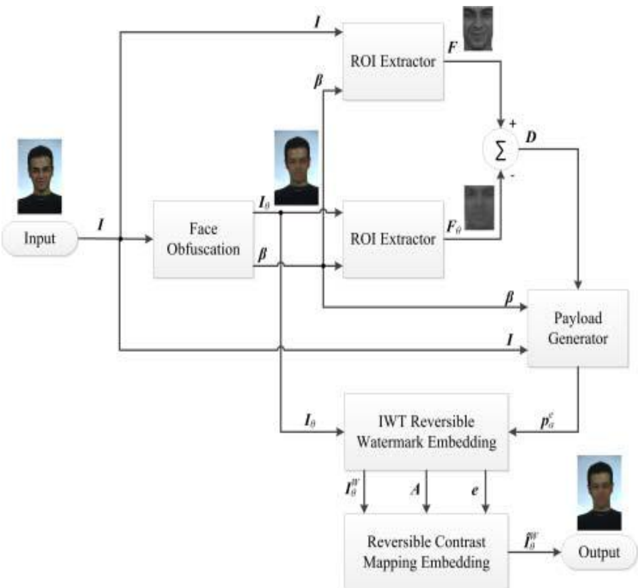
Reversible De-Identification is a process of concealing the identity of individuals, which enables persons in possession of high security credentials to recover the original multimedia content of containing the private information. The system consists of two modules. First an analysis module which identifies and follows regions of interest (ROI's) where faces are detected. Second, the JPEG 2000 encoding module compresses the frames keeping the ROI's in a separate data layer, so that the correct rendering of human faces can be restricted. JPEG 2000 is the new standard for image compression, offers a new flexibility to the coded image. In particular, JPEG 2000 allows differentiating regions of interest from their background. We introduce our view point that privacy and security are not always adversarial goals. We use face detection software to detect the faces in an image or video. an application with some mixture like "skin" detection, text detection, motion detection and /or "voice" detection would equally apply .The basic concept is cryptographic extension of the obscuration idea that has been explored while Senior- et- al did address encryption, their approach requires a special "privacy console" and the encrypted data is out-of-band reprocessed data requiring special equipment, However these methods completely destroy the naturalness of the captured video.

A ROI transform-domain scrambling technique is driven by a Pseudo Random Number Generator (PRNG) which is initialized by a seed value. The seed is encrypted, e.g. using public key encryption, and embedded in the compressed stream as private date. The method is fully reversible. Namely, authorized users, in possession of the secret encryption key, can reverse the scrambling process and recover the truthful scene. The scrambling is confined to ROI, whereas the background remains unaltered. Finally, it has a small impact in terms of coding efficiency, and requires a low computational complexity. There have been several image scrambling schemes for protecting confidentiality of sensitive images basically through cryptographic and Steganographic techniques. An image scrambling scheme basically transforms an image into another unintelligible image. In spite of these efforts, analysis indicates that security level is still not strong for images and multimedia data in general. Also these techniques barely consider the significant intrinsic properties of images. This indicates the need for content-based schemes which are simpler yet stronger for shielding confidentiality of digital images. But the scrambling process better maintains the naturalness of the video. Non-reversible watermarking was adopted to solve the latter issue and embed the information which is needed to recover the De-Identified region within the video itself. Here both these schemes are irreversible and the noise introduced by the watermark embedding process remains permanent, overall compression efficiency is reduced.

This work employs reversible watermarking to solve the former issue. This method induces significant distortions within the obfuscated image themselves. This work presents a Reversible De-Identification method for lossless images. And the approach adopts Reversible Watermarking to make the system reversible. The proposed solution is completely independent from the obfuscation process, and is thus generic. Nonetheless, this work employs the k-Same obfuscation process, which ensures k-anonymity, to obfuscate the face of frontal images. The difference between the original and obfuscated image is compressed, authenticated, encrypted and embedded within the obfuscated image itself. This method keeps the naturalness of the obfuscated images while the original image can only be recovered by individuals having the proper encryption key.

The Reversible Watermarking schemes adopted in this work were found to outperform existing state-of-the-art schemes. Furthermore, experimental results demonstrate that the proposed scheme can recover and authenticate all obfuscated images considered.

2. System Overview



.

Figure 1: Illustrates the schematic diagram of the Forward Reversible De-Identification

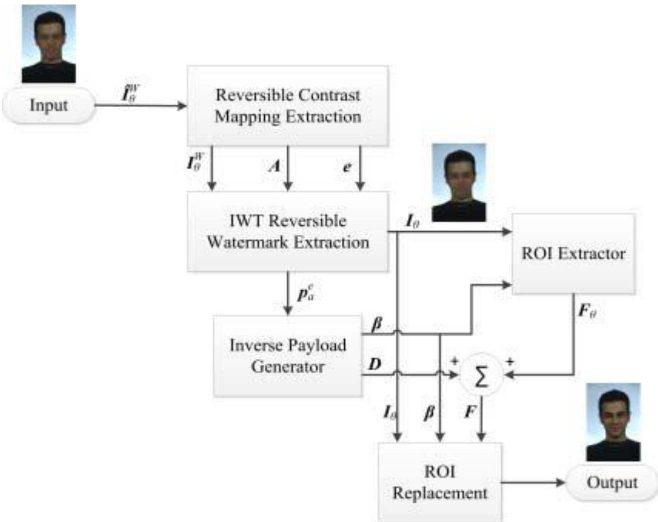


Figure 2: Schematic diagram of the Inverse Reversible De-Identifications Process.

Fig 1 receives the original image I and conceals the face of the person using the Face Obfuscation process to generate an obfuscated image I_Θ. This work considers color images using the YCbCr color space. The coordinates of the top left corner and bottom right corner of the De-identified region is enclosed within the bounding box β, which is passed to both ROI Extraction processes to extract the face image F and the obfuscated face image FΘ. The face images are then subtracted to derive the difference face image D.

The Payload Generator process is then used to convert the difference face image D and bounding box β into a packet p_a^e which is authenticated and encrypted. The packet p_a^e is then embedded within the obfuscated image I_Θ using the Integer Wavelet Transform (IWT) Reversible Watermark Embedding process (1st level) which generates the embedded image I_Θ^w, the auxiliary information A and the residual bitstream 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 (A and e) within the embedded image I_Θ^w, which usually corresponds to few bits, and generates the second level embedded obfuscated image $\hat{I}_\Theta^w$. This method is ideal since it does not need additional information to resolve overflow/underflow issues. Moreover, the distortions introduced at low bitrates are generally negligible. However, its performance significantly degrades at higher bitrates and is therefore not suitable to embed large payloads.

Fig. 2 depicts the schematic diagram of the Inverse Reversible De-Identification process. The second order embedded obfuscated image $\hat{I}_\Theta^w$ is inputted to the Reversible Contrast Mapping Extraction process which extracts the first level embedded obfuscated image I_Θ^w together with the auxiliary information A and the residual bit stream e. The IWT Reversible Watermark Extraction process is then used to extract the original payload p_a^e and original obfuscated image I_Θ. The Inverse Payload Generator reverses the process of the Payload Generator and recovers the difference image D and the bounding box β, which is used by the ROI

Extractor process to extract the obfuscated face F_Θ. The difference image D and obfuscated face F_Θ are then summed to derive the original face F, which is used by the ROI Replacement process to recover the original image I_{rec}. It is important to notice at this stage that the packet p_a^e is authenticated and encrypted, and therefore the difference image D and bounding box β 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.

3. Forward Reversible De-Identification

3.1 Face Obfuscation

The Face Obfuscation process receives the original image 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 and the eye detector 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 β and used to extract the face F which is aligned using affine transformations. The aligned face image 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 F_Θ. The obfuscated face image F_Θ is then realigned to match the orientation of the original face image F using affine transformations and then overwrites the face region in the original image I to derive the obfuscated image I_Θ.

3.2 ROI Extraction

The ROI Extraction process is a simple algorithm which employs the bounding box coordinates β to identify the region to be cropped from the input image I (or I_Θ). The cropped sub-image is then stored in the face image F (or obfuscated face image F_Θ).

3.3 Payload Generator

The Payload Generator Process receives the difference image D which is compressed using the predictive coding method followed by the Deflate algorithm. The original image I is authenticated using SHA-1 which generates a 20-Byte Hash. The Hash will be used by the Inverse Reversible De-Identification process to ensure that it recovers the original image I, and is thus appended to the Payload. The bounding box coordinates β are also required at the receiver to identify the face region and are therefore included as information within the header. The resulting packet pa, illustrated in Fig. 3, was then encrypted using AES-128 to generate the encrypted packet p_a^e .

β	Payload	Hash

Figure 3: The authenticated packet pa.

3.4 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 within I.C represents the capacity needed to embed p_a^e bits and is computed using

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

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 (in our case 3). 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.

3.4.1 Threshold Selection

The proposed Threshold Selection method is based on the observation that different sub-bands provide different levels of distortions. However, in order to reduce the complexity of the optimization function, the following assumptions were made the chrominance sub-bands have similar properties and thus share the same threshold. The HL and LH sub-bands within the same color channel (luminance or chrominance) are assumed to have similar characteristics and therefore have the same threshold.

This work employs Differential Evolution (DE), which is a population based optimization algorithm, to derive the set of threshold which minimize a distortion criterion while ensuring that the capacity of the proposed system is sufficient to embed the message s.

3.4.2 Forward Integer Wavelet Expansion

The Forward Integer Wavelet Expansion process receives the set of thresholds T which are derived by the Threshold Selection process and encapsulates the packet p_a^e shown in Fig. 3 to generate the packet s to be embedded (Fig. 4) .

N_{dec}	T	L	P_a^e

Figure 4: The Actual Bit Stream to Be Embedded ***s***.

The expanded obfuscated image $\mathbf{I}_\theta^w$ is then obtained using the inverse integer wavelet transform. The coordinates of pixels which encounter underflow/overflow issues and their corresponding values are included within the list of auxiliary information ***A***.

3.5 Reversible Contrast Mapping

The only problem with the proposed *Forward Integer Wavelet Expansion* process is that sometimes ***A*** and ***e*** are not empty. This work adopts the syntax shown in Fig. 5 to represent this information r to be embedded. The Flag is a 2-bit field which indicates whether A and 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 A (ore) is signaled in NA (or Ne). The fields NA and Ne are encoded using 8-bits each while the size of A and e are variable length.

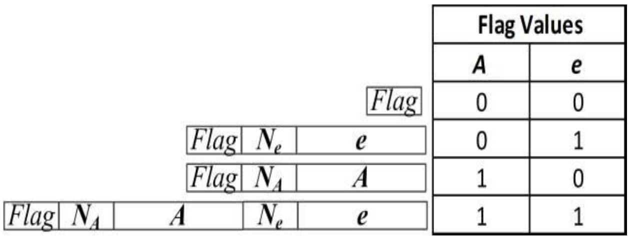


Figure 5: The packet r to be embedded within I_Θ^w

This work adopts the Reversible Contrast Mapping (RCM) to embed the packet ***r*** within the watermarked obfuscated image I_θ^w. 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.

4. Inverse Reversible De-Identification

4.1 Reversible Contrast Mapping Extraction

The *Reversible Contrast Mapping Extraction* process receives the image $\hat{\mathbf{I}}_\theta^W$ and recovers $\mathbf{I}_\theta^W$ and ***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 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 bitstream. More information about this is available in . The auxiliary information ***A*** and residual bitstream ***e*** are then extracted from the packet ***r***.

4.2 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.

4.3 ROI Replacement

The ROI Replacement process replaces the region marked by the bounding box β with the recovered face image F. The image Irec 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

The results presented in this section consider different sets of images. All images considered in this work were converted in the YCbCr color space. To estimate the effectiveness of the proposed Threshold Selection process standard test images were used and to evaluate the whole system frontal images were used. 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 [17]. These results clearly demonstrate that the proposed scheme manages to provide better quality of the stego image $\mathbf{I}_\theta^W$ at different capacities. Simulation results further demonstrate that the proposed scheme needs on average 20 generations to converge. As shown in below fig 6.

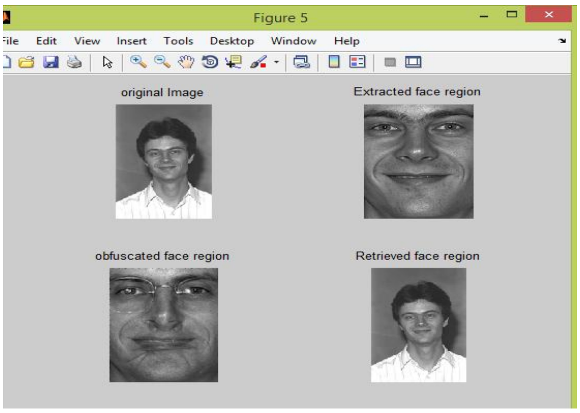


Figure 6: Comparing the resulting reversible de-identified images.

6. Conclusion

Applications that demand for this work are in the field of Medical and Military. This work presents a novel for Face Obfuscation method for lossless compressed images it give optimal set of thresholds and provides a single-pass embedding capacity close to 1.2120 bpp. Further Simulation results proved that this method is able to recover the original image if the correct encryption key is employed. It further shows that 0.3520 bpp were sufficient to cater for 99.8% of the frontal images considered and none of the image needed more than 1.1 bpp.

References

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

Author Profile

Vivek Jaladi has completed his B.E from Basaveshwar Engineering College, Bagalkot in the year 2008 and completed M.Tech in Digital Electronics & Communication from Dayanand Sagar College of Engineering, Bengaluru in 2011. Presently working as Head of the Department of Electronics & Communication Engineering in Lingaraj Appa Engineering College, Bidar. His area of research includes Image Processing, Signal Processing and Networking.

Suhasini Andurey completed her bachelor of engineering in Electronics & Communication Engineering from Guru Nanak Dev Engineering College, Bidar in the year 2013. Currently pursuing M.Tech in VLSI Design & Embedded Systems in Lingaraj Appa Engineering College, Bidar.