FACE OBFUSCATION BASED REVERSIBLE WATERMARKING FOR TAMPER PROOF IRADICATION

Suhasini Andurey[1], Vivek Jaladi[2]

[1]Department of Electronics and Communication Engineering, University College of Engineering, Lingraj Appa college Karnataka India

[2]Asst Prof, Department of Electronics and Communication Engineering, University College of Engineering, Lingraj Appa college Karnataka India

Abstract

This paper proposes a 'Reversible de-identification for tamper proof iradication' using Integer Wavelet Transform that satisfies the requirements of imperceptibility, capacity, and robustness. De-Identification is nothing but a process which is used to ensure privacy by concealing the identity of individuals captured by video surveillance systems. Reversible watermarking also called lossless data hiding it is a method of hiding secret data into cover media, such as digital images, videos, audios, etc. and it enables marked media to be restored to their original form without any distortion. Several reversible watermarking methods have been proposed but one of the 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 paper presents a novel Reversible De-Identification method which can be used in conjunction with any other obfuscation process. To reverse the obfuscation process. The residual information needed is compressed, authenticated, encrypted and embedded within the obfuscated image using a two-level Reversible Watermarking scheme.

Keywords: *Wavelet Transform, imperceptibility, capacity, robustness.*

---***---

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 adoptedn 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 employ 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.

The Forward and Inverse Reversible De-Identification processes are explained in more detail in sections III and IV with the experimental results delivered in section V. The final comments and concluding remarks are drawn in section VI.

2. SYSTEM OVERVIEW

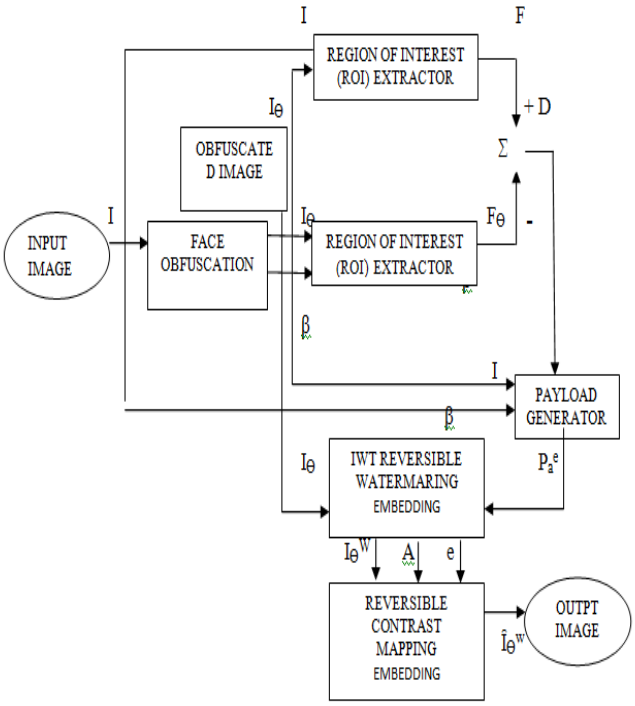

I
F
REGION OF INTEREST (ROI) EXTRACTOR
+D
Iθ
Σ
OBFUSCATED IMAGE
-
Fθ
I
INPUT IMAGE
FACE OBFUSCATION
Iθ
REGION OF INTEREST (ROI) EXTRACTOR
β
I
PAYLOAD GENERATOR
β
Iθ
IWT REVERSIBLE WATERMARING EMBEDDING
Pa^e
Iθ^W
A
e
REVERSIBLE CONTRAST MAPPING EMBEDDING
Îθ^W
OUTPT IMAGE

Fig. 1 illustrates the schematic diagram of the Forward Reversible De-Identification.

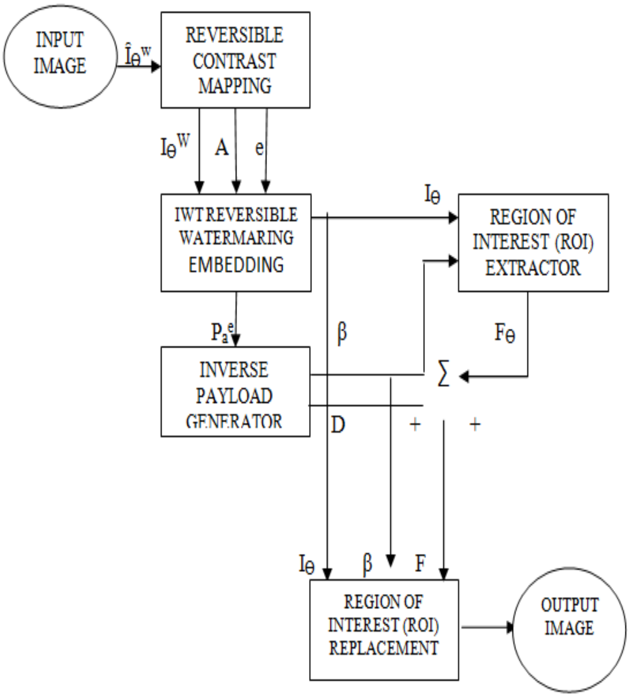

INPUT IMAGE
Îθ^W
REVERSIBLE CONTRAST MAPPING
Iθ^W
A
e
IWT REVERSIBLE WATERMARING EMBEDDING
Iθ
REGION OF INTEREST (ROI) EXTRACTOR
Pa^e
β
Fθ
INVERSE PAYLOAD GENERATOR
Σ
D
+
+
Iθ
β
F
REGION OF INTEREST (ROI) REPLACEMENT
OUTPUT IMAGE

Fig 2. Schematic diagram of the Inverse Reversible De-Identifcation 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 F_Θ. 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 bit stream 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 is 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

Fig 3. The authenticated packet p_a

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 and C represents the capacity needed to embed p_a^e bits and is computed using

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

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.

3.4.4 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. The number of thresholds to be considered by the threshold Selection process and is given by .

$$N_T = 2(1+N_{dec)}$$

In order to clarify this, consider a single level of decomposition. In this case NT = 4 where T1 is the threshold for coefficients in sub-band HH1 of the luminance component, T2 is the threshold for coefficients in sub-band HL1 and LH1 of the luminance component, T3 is the threshold for coefficients in sub-band HH1 in the chrominance components (Cb and Cr) and T4 is the threshold for coefficients in sub-bands HL1 and LH1 in the chrominance components. Note that the subscript for the sub-bands represents the level of decomposition. The thresholds corresponding to sub-bands at higher level of decomposition are considered to be the same for the same color component. Therefore, if we consider a second level of decomposition (NT = 6), the additional threshold T5 controls the coefficients in sub-bands HH2, HL2 and LH2 for the luminance component while threshold T6 is responsible for the coefficients in sub-bands HH2, HL2 and LH2 for the chrominance components. The same happens for higher levels of decompositions. One naive approach is to use exhaustive search to find the optimal set of thresholds. However, this has a time complexity of the order of O(nNT) where n represents the search range. An alternative approach is to use a meta heuristic approach to solve this optimization problem.

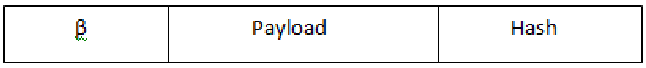
This work employs Differential Evolution (DE), which is a population based optimization algorithm, to derive the set of threshold which minimize a distortion criterion while ensuring that the capacity of the proposed system is sufficient to embed the message s. The time complexity provided by this scheme is of the order of O(G×NP×NT), where NP is the population size and G corresponds to the number of generations.

Differential Evolution starts with a random set of possible solutions and tries to find better solutions through mutation and cross-over. The set of potential thresholds Δ is a list of threshold NP vectors which are initialized using a uniformly distributed random number generator. The threshold vectors T Δi which do not provide enough capacity are pruned and replaced by another random vector which satisfies it. The population of thresholds evolves over a number of generations using mutation and cross-over. The mutation process generates a mutant vector for every threshold vector contained within the population of NP vectors.

3.4.2 Forward Integer Wavelet Expansion

The Forward Integer Wavelet Expansion process receives the set of thresholds T.

Threshold Selection process and encapsulates the packet p_a^e shown in Fig. 3 to generate the packet s to be embedded as shown in fig 4 below:



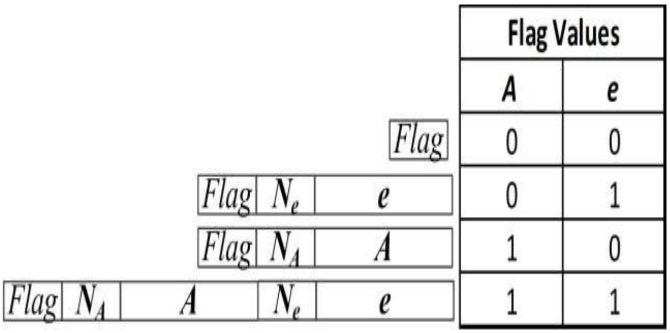
β	Payload	Hash

Fig 4 The authenticated packet ***pa***

The expanded obfuscated image $\boldsymbol{I_\theta}^w$ 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 signalled 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.



	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

Fig 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 $\boldsymbol{I_\theta}^w$ 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

Each block of Fig 2 is discussed below:

4.1 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 ***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 ***A*** and residual bit stream ***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 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 6 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 correspond 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 ***e*** was empty for 99.8% of the time and the Auxiliary information ***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.

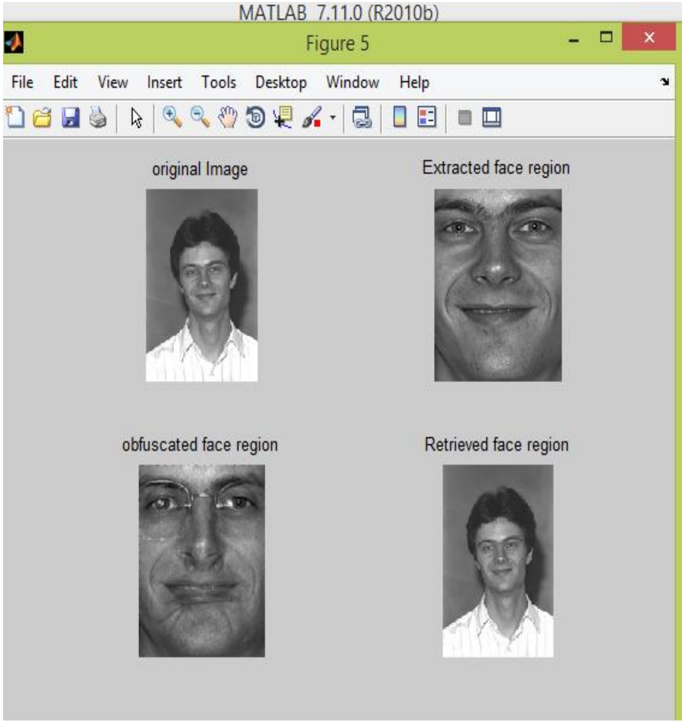


Fig 6 Comparing the resulting reversible de-identified images (a) Original Image, (b) Scrambling of DCT coefficients , (c) Encryption of pixel values and (d) proposed method.

6. FUTURE WORK

Comparing the resulting reversible de-identified images using LAB transformation since it is superior than the color transformation used in my existing paper.

7. 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.

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.

[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]. K. Martin and K.N. Plataniotis, "Privacy protected surveillance using secure visual object coding," IEEE Trans. Circuits and System for Video Technol., vol. 18, no. 8, pp. 1152-1162, Aug. 2008.

[7]. 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.

[8]. F. Dufaux and T. Ebrahimi Scrambling for privacy protection in video surveillance systems, "Scrambling for privacy protection in video surveillance systems," in IEEE Trans on Circuits and Systems for Video Technol., vol. 18, no. 8, pp. 1168-1178, Aug. 2008.

[9]. H. Sohn, W. De Neve and Y-M. Ro, "Privacy protection in video surveillance systems: Analysis of subband-adaptive scrambling in JPEG XR," in IEEE Trans. Circuits and Systems for Video Technol., vol. 21, no. 2, pp. 170-177, Feb. 2011.

[10]. J. Meuel, M. Chaumont and W. Puech, "Data hiding in H.264 video for lossless reconstruction of region of interest," in European Signal Processing Conf., Poznan, Poland, Sep. 2007.

[11]. S.S. Cheung, J.K. Panichuri and T.P. Nguyen, "Managing privacy data in pervasive camera networks," in IEEE Int. Conf. on Image Processing, San Diego, California, USA, Oct. 2008.

[12]. P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in IEEE Proc. Computer Vision and Pattern Recognition,Kauai, USA, Dec. 2001.

[13]. F. Hahmann, G. Boer and H. Schramm, "Combination of Facial Landmarks for Robust Eye Localization using the Discriminative Generalized Hough Transform," in Int. Conf. of the Biometrics Special Interest Group, Darmstadt, Germany, Sep. 2013.

[14]. R. C. Gonzalez and R.E. Woods, Digital Image Processing, Second Edition, Prentice Hall, 2001.

[15]. M. Weinberger, G. Seroussi and G. Sapiro, "LOCO-I: A Low Complexity, Context-Based, Lossless Image Compression Algorithm," in Proc. IEEE Data Compression Conf., Washington DC., USA, Apr. 1996.

[16]. P. Deutsch, DEFLAGE Compressed Data Format Specification version 1.3, RFC1951 (International), May 1996.

[17]. G. Xuan, Y.Q. Shi, P. Chai, X. Cui, Z. Ni and X. Tong, "Optimum Histogram Pair based image Lossless Data Embedding," in Proc. Int. Workshop on Digital Watermarking, Berlin, Germany, 2008.

[18]. Z. Wang, E.P. Simoncelli and A.C. Bovik, "Multi-Scale Structural Similarity for Image Quality Assessment, in IEEE Proc.Asilomar Conf. on Signals, Systems and Computers, Pacific Grove, CA, USA, Nov. 2003.

[19]. R. Storn, K. Price, "Differential Evolution: A simple and efficient heuristic for global optimization over continuous spaces," J. on Global Optimization, vol.11, no. 4, pp. 341-359, Dec. 1997.

[20]. F. De Simone, M. Ouaret, F. Dufaux, A.G. Tescher and T. Ebrahimi, "A Comparative study of JPEG2000, AVC/H.264 and HD Photo," in Proc. SPIE Optics and Photonics, Applications of Digital Image, San Diego, USA, Aug. 2007.

[21]. D. Coltuc and J-M. Chassery, "Very Fast Watermarking by reversible Contrast Mapping," IEEE Sig. Proc. Letters, vol. 14, no. 4, Apr. 2007.

[22]. T. Ahonen, A. Hadid and M. Pietikainen, "Face Description with Local Binary Patterns: Application to Face Recognition," in IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp. 2037-2041, Dec. 2006.