Multimed Tools Appl (2013) 67:593–606
DOI 10.1007/s11042-012-1037-9

Joint watermarking and encryption for still visual data

Nidhi Taneja · Gaurav Bhatnagar · Balasubramanian Raman · Indra Gupta

Published online: 17 March 2012

Abstract Joint watermarking and encryption is an upcoming security solution that combines leading but complementary techniques to achieve an enhanced security level. Real time applications using joint watermarking and encryption framework has three requirements: data to be efficiently compressed, watermarking technique to sustain compression, and encryption technique to be developed in a way so as not to disturb the compression efficiency. Finding an optimal solution that combines the three techniques while fulfilling these requirements is a challenging problem. This paper thus, proposes a wavelet domain based joint watermarking and encryption framework that employs singular value decomposition based watermark embedding and sign bit encryption prior to compression. The varying significance of different subbands has been considered to encrypt the data without adversely effecting the compression ratio. Experimental analysis using various evaluation parameters and attack scenarios has revealed the ability of the proposed framework to prove content-ownership, even from the encrypted data. Comparative analysis with the existing techniques reflect its ability to provide better security with less computational

N. Taneja (✉) · I. Gupta
Department of Electrical Engineering, Indian Institute of Technology Roorkee,
Roorkee 247 667, India
e-mail: nidhi.iitr@gmail.com

I. Gupta
e-mail: indrafee@iitr.ernet.in

G. Bhatnagar
Department of Electrical and Computer Engineering, University of Windsor,
Windsor, ON, Canada
e-mail: goravdma@iitr.ernet.in

B. Raman
Department of Mathematics, Indian Institute of Technology Roorkee,
Roorkee 247 667, India
e-mail: balarfma@iitr.ernet.in, balaiitr@ieee.org

resources. This makes it a preferable solution for data security at all stages of data archival, transmission or distribution.

Keywords Joint watermarking and encryption · Singular value decomposition · Set partitioning in hierarchical trees

1 Introduction

With the advancements in the field of communication, coding and networking technology, multimedia applications have increased in day-to-day life. This technological advancement has also equipped potential attackers with the tools to illegally copy, manipulate, or distribute digital data. Hence, security technqiues have become an integral component of data archival, transmission or distribution. This has led to the development of various techniques covered under the umbrella of digital rights management [2, 3, 5–7, 9].

Among the several digital rights management techniques, encryption [13, 16] and watermarking [8, 20] are considered as the first and second line of defence, respectively. The former ensures confidentiality by making the data unintelligible for an unauthorized user, whereas the latter provides copyright protection by embedding a watermark into media data.

Though these two techniques have been developed independently and are complementary to each other, they have been integrated for secure data storage or transmission [10–12, 19, 21]. Their integration not only provides data confidentiality but also proves content ownership at all stages of data consumption. Wu et al. proposed to selectively watermark MPEG data and then encrypt watermarked data [21]. Simitopoulos et al. proposed to embed the watermark in quantized DCT coefficients prior to I-frame encryption using IDEA [19].

To save computational resources, Lian et al. proposed commutative watermarking and encryption technique that perform both these operations in a single step [10]. After identifying varying significance of different parts of image data, middle level wavelet coefficients have been used for watermark embedding, and remaining coefficients (low and high level) for AES encryption. This has also been extended to MPEG data, where residual, MVD and IPM frames are selected for watermarking and encryption, respectively [11]. However, commutative watermarking and encryption is prone to replacement attack due to the mutually exclusive watermarking and encryption data components [12]. A quasi-commutative approach of watermarking and encryption is thus proposed that watermarks and encrypts the entire data to make joint watermarking and encryption (JWE) framework cryptographically secure [12].

Though several frameworks, integrating the two techniques have been developed; it is still in its infancy stage [1, 10–12, 19, 21]. Joint watermarking and encryption (JWE) frameworks are being developed, researched and discarded at a fast pace. Several intricacies are observed in the JWE framework owing to the fact that compression, which is an integral part of encryption, is a potential attack for the embedded watermark.

For a secure multimedia system, an optimal JWE framework requires a clever interweaving of encryption, watermarking and compression. An efficient JWE frame-

work should provide robustness to the embedded watermark against compression without deteriorating the compression efficiency.

The present work, thus, intends to develop a JWE framework that achieves data confidentiality, proves content ownership and offers high compression ratio. In the proposed framework, watermarking and encryption are implemented at content owner and content distributor end, respectively. To achieve the desired objectives, watermark is embedded using singular value decomposition of the wavelet packet transformed image and encryption is performed during SPIHT encoding. Security attained by the proposed JWE framework is ascertained by detailed experimental analysis.

2 Singular value decomposition

Singular value decomposition (SVD) is a powerful technique in many matrix computations and analyses [4]. Use of SVD in matrix computations provides robustness provides robustness against numerical errors. SVD of a square or a rectangular matrix of size $M \times N$ can be expressed as

$$A = U * S * V^T \tag{1}$$

where U and V are orthogonal (unitary) matrices, and S is a diagonal matrix given by $S = diag(\sigma_1, \sigma_2, ..., \sigma_r)$. Here, σ_i denotes singular value of matrix A, and $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_r$, $1 \leq i \leq r$ and $r = \min(M, N)$. The first r columns of V and U are termed as right and left singular vectors, respectively.

The main motivation for using the SVD is its energy compaction property and its ability to adapt to the variations in local statistics of an image. Each singular value of the image matrix specifies luminance of the image layer, while corresponding pair of singular vectors specify geometry of the image layer. Therefore slight variations of singular values does not affect visual perception of the cover image.

Also, storing the approximation of a matrix using SVD often results in a significant savings over storing the whole matrix. Singular values of a matrix possess algebraic and geometric invariance to some extent, due to which it has certain distinct advantages in digital image processing. For instance, singular values of an image matrix remain same, irrespective of the transposition, rotation or translation performed on the original matrix. Further, singular values of an image are less effected in case of general image processing operations on the image matrix.

3 Proposed joint watermarking and encryption framework

In the proposed JWE framework, the original image X is initially watermarked using key K_w. This watermarked image is then partially encrypted with key K_e. The final image obtained by implementing these two processes in a sequential manner is mathematically expressed as

$$Y = W(X, B, K_w) \tag{2}$$

$$Z = E(Y, K_e) \tag{3}$$

Here, Y, B, K_w, $W()$, Z, K_e and $E()$ are the watermarked copy of original image X, watermark, watermark key, watermark embedding algorithm, encrypted copy of watermarked component Y, encryption key and encryption algorithm, respectively.

The watermarking key, K_w comprises of watermark strength, α^θ as the main key component. This controls perceptibility of the embedded watermark; higher the value of α^θ, more observable is the watermark. An optimal value can be chosen as per the desired visibility of embedded watermark. In contrast, the encryption key, K_e consist of the compression ratio, number of Arnold iterations for scrambling and a seed value for generating a random vector.

A block diagram depicting the proposed JWE framework is indicated in Fig. 1 and the two processes controlled by the independent keys, K_w and K_e, are explained as follows.

The watermarking process initially transforms the host image into wavelet packet transform (WPT) domain. SVD is then performed on all subbands of the transformed image and the watermark image. For watermark embedding, the obtained singular values are modified using (4)

$$(\sigma_{f_{l,\,p}^{\,\theta}})^* = \sigma_{f_{l,\,p}^{\,\theta}} + \alpha^\theta\, \sigma_W \tag{4}$$

where $\sigma_{f_{l,\,p}^{\,\theta}}$ gives original singular values of the subband, $(\sigma_{f_{l,\,p}^{\,\theta}})^*$ denotes modified singular values of the subband, σ_W denotes singular values of the watermark image, and α^θ is the watermark strength.

After replacing original singular values by the modified values, inverse SVD is taken. This is followed by inverse WPT to retrieve the watermarked image. This watermarked image is transmitted to the content distributor end. Thereafter, encryption is performed on this watermarked image during SPIHT compression [17].

In SPIHT compression, an image is initially transformed into wavelet domain, and a tree structure is formed. The tree structure is then encoded to obtain a SPIHT compressed bitstream. In the proposed framework, encryption is implemented in wavelet domain, just before the formation of tree structure. Encryption is achieved by scrambling the approximation subband using Arnold cat map [15]. This is followed by sign bit encryption of the scrambled transform coefficients using a stream cipher,

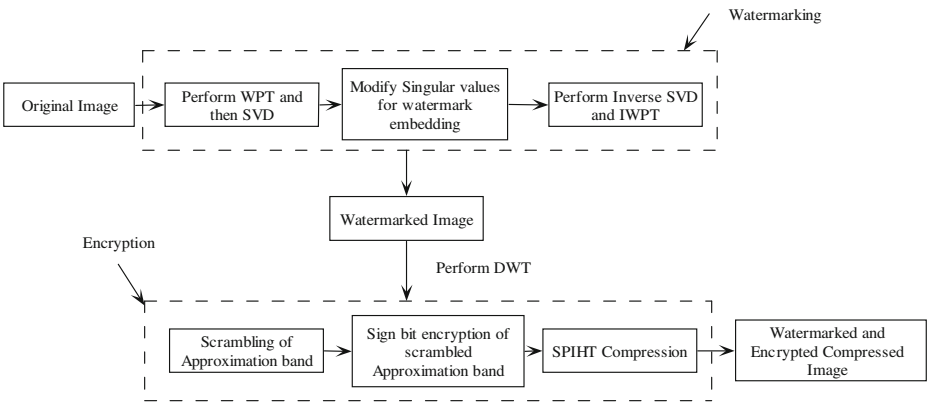

Fig. 1 Block diagram for the proposed framework

generated from a seed value. The original approximation subband is replaced with the scrambled and sign bit encrypted subband. Afterwards, the modified transformed image is used to generate the compressed bitstream using SPIHT.

At the receiver end, compressed bitstream generates the transformed image and inverse DWT of this transformed image provides the reconstructed image. An unauthorized receiver, not having the security keys, would only retrieve an incomprehensible image. Contrary to this, an authorized receiver would perform sign bit decryption and Arnold descrambling of the approximation subband before IDWT. This provides a correctly decrypted output to an authorized receiver. To verify achieved security level of the proposed framework, several experiments have been performed, and are discussed in the next section.

4 Results and discussion

The proposed framework provides twin layer of protection to digital images by combining watermarking and encryption. To substantiate performance of the proposed framework, different subjective and objective evaluation parameters are used. Diverse watermarking and encryption related security attacks are also launched to assess robustness of the proposed framework. Simulations have been performed on various grayscale images, however, results for only 'Barbara' image are illustrated here.

4.1 Subjective and objective evaluation

To examine the quantum of detail actually lost, or retained by the proposed JWE framework, a visual inspection of the watermarked and encrypted images is performed. These images are illustrated in Fig. 2. It is observed that the watermarked

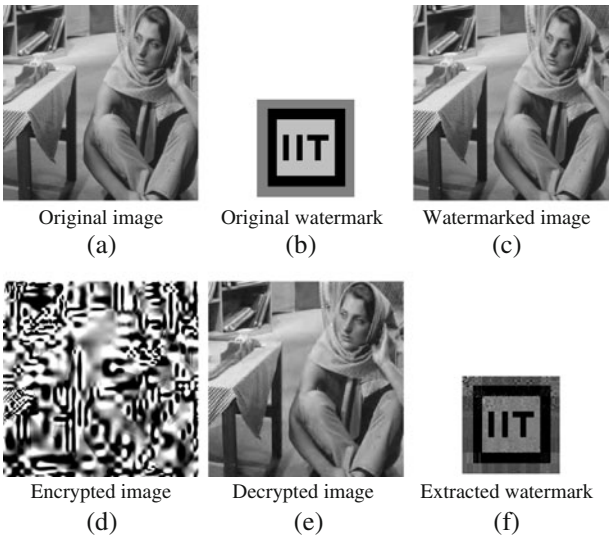

Fig. 2 Results for the proposed framework

Table 1 PSNR (dB) obtained for various images

Image	Barbara	Lena	Plane	Crowd	Bridge	Lake
Watermarked	40.1201	38.7121	38.9503	39.5840	37.5025	37.2499
Encrypted	3.2341	3.1203	3.1842	3.0001	3.1981	2.9064

image is similar to the original image, and the encrypted image is completely incomprehensible. The embedding of watermark in an imperceptible manner has not resulted into loss of any detail from the original image. In contrast, an unintelligible encrypted image reflects that the developed encryption technique provides high data confidentiality and does not leak any information of the original image. To further verify the results, objective evaluation is performed using peak signal to noise ratio (PSNR).

The obtained PSNR values for the watermarked and the encrypted output with reference to the original image are indicated in Table 1. A high PSNR value after watermarking indicates perceptual similarity between the original and the watermarked image, while a low PSNR value of the encrypted output indicates sufficient dissimilarity between the original and the encrypted image. This indicates more computational effort required by an intruder to retrieve the correct image without the knowledge of security keys. PSNR values and visual inspection of results depicts that the proposed technique satisfies the subjective and objective evaluation metric for an acceptable watermarking and encryption technique.

4.2 Key sensitivity analysis

As per the Kerckhoff's principle, security keys are the most important part of any cryptosystem, and decryption using an incorrect key or an approximately correct key should not reveal any details of the original image [18]. To determine key sensitivity of the proposed encryption technique, wrong decryption keys are generated by introducing slight modifications in Arnold scrambling iterations and the seed value. Decryption is then performed by using these slightly modified keys. Figure 3a and c demonstrates the decrypted results when incorrect descrambling iterations or incorrect seed value is considered. It is observed that the images decrypted with wrong decryption keys do not give a clear view of the original image. This reflects high key sensitivity of the developed encryption algorithm.

Thereafter, watermark is extracted from these incorrectly decrypted images. The extracted watermarks are shown in Fig. 3b and d. It is observed that despite unintelligible decrypted images, meaningful watermarks are extracted. This reflects robustness of the watermark embedding technique. To further verify strength of embedding technique, watermark is extracted from the encrypted image. The extracted watermark is indicated in Fig. 3f, and can easily be related to the original watermark.

Strength of the encryption technique is evident from achieved data confidentiality and high key sensitivity. In addition to this, extraction of watermark from the encrypted and incorrectly decrypted image illustrates strength of the watermarking technique. This depicts that content ownership can be proved in a scenario, where a

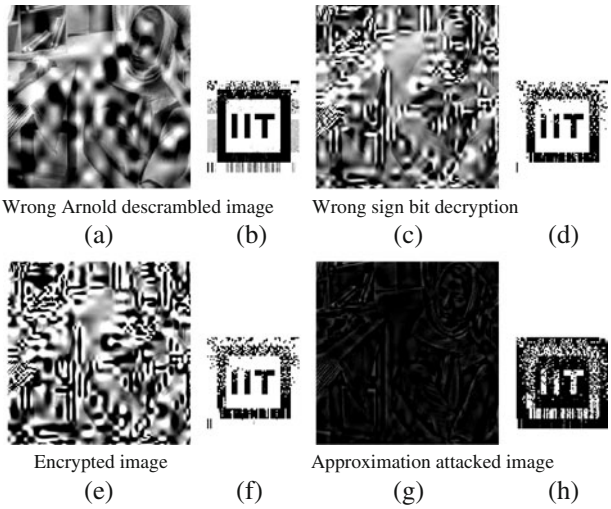

Fig. 3 Key sensitivity results for the encryption technique

pirate captures an unclear but watermarked copy of the original image. The above analysis corroborates strength of the developed JWE framework.

4.3 Compression performance analysis

In the proposed JWE framework, compression ratio achieved by the employed SPIHT encoder is analyzed. To experimentally evaluate the effect on compression efficiency, original and encrypted images are compressed with 0.8 bits per pixel. As the output bit rate is equal for both the images, length of the compressed bitstream is observed to be same for all the original and the encrypted image. This indicates that the proposed framework does not adversely effect compression efficiency of the SPIHT encoder.

4.4 Approximation attack

Security of the proposed technique is also verified against approximation attack [14]. In this attack, part of the encrypted data is replaced by random data and reconstruction is performed using this partially assumed data. In the present case, few transform coefficients of approximation subband are replaced by a constant value '0', before IDWT. Figure 3g and h shows the reconstructed image and the extracted watermark for this case. It is observed that a clear view of the original image is not obtained. However, watermark extracted from this approximate image has perceptual resemblance with the original watermark. This indicates resistance of the proposed framework for approximation attack.

An approximated copy of the test image is used to measure block-based Luminance Similarity Score (LSS), which captures the coarse luminance information [14]. LSS measures the perception-oriented distance between the clear-text copy of

multimedia and attacker's recovered copy from the encrypted media. It was assumed that two given images are pre-processed to be aligned and scaled to the same size. These two images are first divided into blocks in the same way, using 8×8 or 16×16 non-overlapping blocks. Average luminance values of ith block is then calculated from both images to measure LSS using

$$LSS \cong \frac{1}{N} \sum_{i=1}^{N} f(x_{1i}, x_{2i}) \tag{5}$$

Here, the function $f(x_1, x_2)$ for each pair of average luminance values is defined as

$$f(x_1, x_2) = \begin{cases} 1, & \text{if } |x_1 - x_2| < \frac{\beta}{2} \\ -\alpha \; round\left(\frac{|x_1 - x_2|}{\beta}\right), & \text{otherwise} \end{cases} \tag{6}$$

where the parameters α and β control sensitivity of LSS and set to 0.1 and 3, respectively. For the proposed framework, negative LSS is obtained. This indicates a substantial dissimilarity in luminance of the two images.

4.5 Attack analysis

After performing key sensitivity and approximation attack analysis for the proposed encryption technique, this section discusses performance of the proposed watermarking technique in different attack scenarios. Robustness of the proposed watermarking technique is investigated by launching various attacks on the watermarked image, and observing the quality of extracted watermarks from the attacked images. Visual inspection of the extracted watermark is performed to assess its perceptual similarity with the original watermark. For an objective evaluation of similarity, correlation coefficient is calculated between the extracted and actual singular values, using

$$\rho(w, \bar{w}) = \frac{\sum_{i=1}^{r} (w(i) - w_{\text{mean}})\,(\overline{w}(i) - \overline{w}_{\text{mean}})}{\sqrt{\sum_{i=1}^{r} (w(i) - w_{\text{mean}})^2} \sqrt{\sum_{i=1}^{r} (\overline{w}(i) - \overline{w}_{\text{mean}})^2}} \tag{7}$$

where w, $\overline{w}$, w_{mean} and $\overline{w}_{\text{mean}}$ are the original singular values, extracted singular values, mean of the original singular values and mean of the extracted singular values. Here, $r = \min(M, N)$, and (M, N) denote size of the image.

Among the various attacks launched on the watermarked image, basic attack includes (a) a 13×13 Gaussian blurring on the watermarked image, (b) rotation of the watermarked image by 50°, and (c) addition of 80% Gaussian noise to the watermarked image. Watermarks are extracted from these three attacked images. Figure 4c–e indicates the attacked watermarked images and their corresponding extracted watermarks. It is observed that the extracted watermarks are recognizable and can be assumed as a degraded version of the original watermark. Correlation coefficient values for the extracted watermarks is indicated in Table 2.

As cropping is a frequently used operation in image applications, watermarked image is also tested for cropping attack. Process of selecting and removing a portion of an image is generally performed to create focus or strengthen the composition. In the present test case, the watermarked image is cropped to only 2.5% of the actual

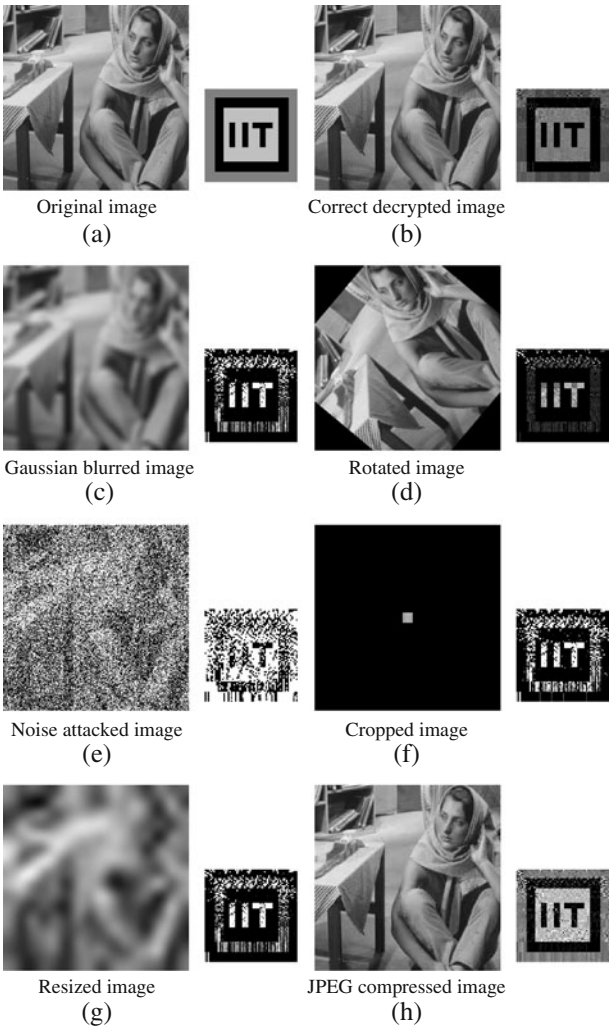

Fig. 4 Image and its extracted watermark

size, and watermark extraction is performed. Figure 4f indicates the cropped image and the extracted watermark. It is to be noted that the watermark could be extracted, even from an image equal to 2.5% of the actual image size.

Another frequently used image processing operation is resizing, wherein the image is reduced or enlarged to a desired size. This leads to data loss of the original

Table 2 Correlation coefficient (CC) for extracted watermark from attacked Barbara image

Attack	Gaussian Blur	Rotation	Noise	JPEG compression	Resizing	Cropping
CC	−0.6885	−0.9402	0.3732	0.9656	−0.6832	−0.6079

image and the watermark embedded within it. In the present test case, the image is reduced to 16 × 16 and again carried back to the original size 256 × 256. Figure 4g depicts the resized image and its corresponding extracted watermark. It is observed that the extracted watermark is still recognizable and is similar to the original watermark.

Another potential attack for a watermarking technique is compression, that is generally performed owing to the large data size and limited channel bandwidth. As image compression techniques are lossy in nature, they lead to data loss from the entire image and the watermark embedded in it. Despite the losses, a secure system requires that the watermark is extractable, even from a compressed image.

To assess the proposed technique against compression attack, lossy JPEG compression, with a compression ratio of 80:1, is performed on the watermarked image. Watermark is extracted from this JPEG compressed image. Figure 4h illustrates the JPEG compressed image and its extracted watermark. It is observed that the extracted watermark is of very high quality, and almost an exact replica of the original watermark. Further, it is to be noted that the proposed framework is based on SPIHT compression of the watermarked data. Hence, the watermark indicated in Fig. 4b is actually the watermark extracted from a SPIHT compressed image. This demonstrates robustness of the proposed watermarking technique against SPIHT compression. This reflects that the proposed watermarking technique can withstand lossy JPEG and SPIHT compression attack.

In all the above-mentioned attack scenarios, it is observed that the extracted and the original watermark are perceptually similar. This, along with the correlation coefficient values indicated in Table 2, reflects the resistance of the proposed watermarking technique against various image processing operations. The above-discussed analysis reflects the ability of the proposed framework to prove content ownership, even from attacked and compressed images.

5 Comparative analysis

This section discusses comparative analysis of the proposed framework, with an existing JWE framework [10]. The existing framework utilizes the entire image data to provide data confidentiality. It provides AES encryption to all the coefficients of low level subband, and sign bit encryption to all the coefficients of remaining subbands. In contrast, the proposed framework performs only sign bit encryption

Table 3 Scheme of existing and proposed JWE

Technique	Watermarking	Encryption
Existing [10]	All coefficients of middle level subband are used, i.e., ($M_1 \times N_1$) coefficients used for a subband of size ($M_1 \times N_1$)	AES in approximation subband and sign bit encryption in remaining subbands
Proposed	Uses only singular values for watermarking i.e., min. (M_1, N_1) coefficients used for a subband of size ($M_1 \times N_1$)	Scrambling and sign bit encryption of only approximation subband

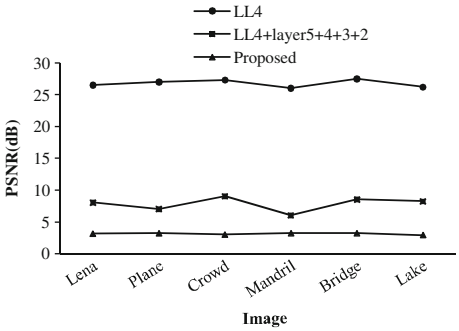

Fig. 5 PSNR comparison chart

for coefficients of the approximation band. This drastically reduces the amount of data encrypted in the proposed technique.

Further, existing technique uses all the coefficients of middle level subband for watermarking [10]. The proposed framework, however, performs watermark embedding, only in the singular values of the subband. As singular values form a diagonal matrix, thus, for a subband of size $(M_1 \times N_1)$, the coefficients used for watermarking with the proposed technique are expressed as $\min.(M_1, N_1)$. This reflects a drastic reduction in computational requirements, as compared to $(M_1 \times N_1)$ coefficients, that are used for the existing technique [10].

A comparative representation for the amount of data used for watermarking and encryption is indicated in Table 3. Apart from the amount of data used, existing and proposed techniques are also compared on the basis of attained PSNR value. A comparative graph for PSNR value of the proposed and existing techniques is depicted in Fig. 5. This reveals low PSNR value achieved by the proposed framework, which is analogous to high data confidentiality.

To summarize, comparative analysis indicate that despite the small quantum of data watermarked and encrypted in the proposed framework, PSNR obtained is better than the existing techniques.

6 Conclusion

JWE is emerging as an effective security solution, that provides data confidentiality and proves content ownership. Compression is necessary for encryption; however, it behaves as an attack for the embedded watermark. In such a scenario, obtaining an optimal solution is a dexterous task.

A novel JWE framework is thus presented that performs watermarking and encryption in an independent manner at the content owner and distributor end, respectively. In the proposed framework, watermark is embedded in the wavelet packet domain using SVD, and the watermarked image is partially encrypted during SPIHT compression. Thorough performance analysis reflects the robustness of the proposed framework to withstand compression, approximation and various other image processing attacks. The developed framework does not adversely effect the

compressibility of the SPIHT encoder. The ability to prove content ownership, even from a compressed, encrypted, or an attacked image is also validated. Thus, it acts as a two-fold impediment to illegal distribution of media data, and a preferable choice for secure image transmission or distribution.

References

1. Boato G, Conci N, Conotter V, De Natale FGB, Fontanari C (2008) Multimedia asymmetric watermarking and encryption. Electronics Lett 44(9):601–602
2. Chang FC, Huang HC, Hang HM (2007) Layered access control schemes on watermarked scalable media. J VLSI Signal Process Syst Signal Image Video Technol 49(3):443–455
3. Committee on Intellectual Property Rights in the Emerging Information Infrastructure (2000) The digital dilemma: intellectual property in the information age. US National Research Council, National Academic Press, Washington, D.C.
4. Dewilde P, Deprettere EdF (1988) Singular value decomposition. An introduction. In: Deprettere EdF (ed) SVD and signal process.: algorithms, applications, and architectures. Elsevier Science Publishers, North Holland, pp 3–41
5. Eskicioglu AM (2003) Protecting intellectual property in digital multimedia networks. IEEE Comput 36(7):39–45
6. Eskicioglu AM (2003) Multimedia security in group communications: recent progress in key management, authentication, and watermarking. Multimedia Syst 9:239–248
7. Huang HC, Chen YH (2009) Genetic fingerprinting for copyright protection of multicast media. Soft Comput 13(4):383–391
8. Kundur D, Hatzinakos D (2004) Towards robust logo watermarking using multiresolution image fusion. IEEE Trans Multimedia 6(1):185–197
9. Li B, He J, Huang JW, Shi YQ (2011) A survey on image steganography and steganalysis. J Inf Hiding Multimedia Sig Proc 2(2):142–172
10. Lian S, Liu Z, Zhen R, Wang H (2006) Commutative watermarking and encryption for media data. Optical Engg Lett 45(8):1–3
11. Lian S, Liu Z, Ren Z, Wang H (2007) Commutative encryption and watermarking in video compression. IEEE Trans Circuits Syst Video Technol 17(6):774–778
12. Lian S (2009) Quasi-commutative watermarking and encryption for secure media content distribution. Multimed Tools Appl 43(1):91–107
13. Liu J-L (2006) Effective selective encryption for Jpeg2000 images using private initial table. Pattern Recogn 39:1509–1517
14. Mao Y, Wu M (2006) A joint signal processing and cryptographic approach to multimedia encryption. IEEE Trans Image Process 15(7):2061–2075
15. Peterson G (1997) Arnold's cat map. Available from: http:online.redwoods.cc.ca.us/instruct/darnold/maw/catmap3.htm
16. Pommer A, Uhl A (2003) Selective encryption of wavelet-packet encoded image data: Efficiency and security. Multimedia Syst 9(3):279–287
17. Said A, Pearlman WA (1996) A new, fast, and efficient image codec based on set partitioning in hierarchical trees. IEEE Trans Circuits Syst Video Technol 6(3):243–250
18. Schneier B (1995) Applied cryptography second edition: protocols, algorithms, and source code in C. Wiley, New York
19. Simitopoulos D, Zissis N, Georgiadis P, Emmanouilidis V, Strintzis MG (2003) Encryption and watermarking for the secure distribution of copyrighted MPEG video on DVD. Multimedia Security 9(3):217–227
20. Su K, Kundur D, Hatzinakos D (2005) Statistical invisibility in collusion-resistant digital video watermarking. IEEE Trans Multimedia 7(1):43–51
21. Wu T, Wu S (1997) Selective encryption and watermarking of MPEG video. In: Proc. int. conf. image science, systems and technology. Ontario, Canada

Nidhi Taneja received her B.E. Degree in Electronics & Communication and M.Tech Degree in Digital Communication in 2001 and 2006, respectively. She has received her Ph.D. in Electrical Engineering at Indian Institute of Technology Roorkee, India. At present, she is an Assistant Professor in Department of Electronics and Communication Engineering at Delhi Technological University (Formerly Delhi College of Engineering), New Delhi. Her area of interest includes Wireless Communication, Multimedia Transmission over Packet Networks, Image Encryption, Watermarking, Biometrics and Visual Cryptography.

Gaurav Bhatnagar received his Ph.D. in Mathematics from Indian Institute of Technology Roorkee. At present, he is a post-doctoral fellow in Department of Electrical and Computer Engineering at University of Windsor, Canada. He has several research papers in various reputed international journal and conferences. His areas of research include Image Analysis, Image Fusion, Biometrics, Wavelet Analysis, Cryptography and Digital Watermarking.

Balasubramanian Raman received his Ph.D. in Mathematics (2001) from Indian Institute of Technology, Madras, India. At Present, he is an Assistant Professor and Head of the Computer Vision, Graphics and Image Processing Laboratory in the Department of Mathematics at Indian Institute of Technology Roorkee, India. He worked as a Post Doctoral Associate in ECE Department, and member of the Visualization Research Laboratory (VIZ Lab), at Rutgers, The New State University. He was also a Post Doctoral fellow of Computer Engineering and Computer Science (CECS), and member of the Computational Intelligence Research Laboratory (CIRL), at the University of Missouri-Columbia (MU), Missouri, USA. He has also worked as Visiting Professor in Department of Electrical and Computer Engineering at University of Windsor, Canada under Boyscast Fellowship. His area of research includes Computer Vision, Graphics, Satellite Image Analysis, Scientific Visualization, Imaging Geometry, Reconstruction Problems, Image Encryption and Digital Watermarking.

Indra Gupta received her B.Tech. Degree in Electrical Engineering from HBTI, Kanpur, in 1984. She completed her M.E. and Ph.D. from University of Roorkee, India. Currently, she is an Associate Professor in the Department of Electrical Engineering, Indian Institute of Technology Roorkee, India. Her areas of interest includes Advanced Microprocessor Applications, Information Security, Multimedia Processing, Process Control Applications, Biomedical Imaging, Content based Image Retrieval and Online Computer Applications.