Signal Processing: Image Communication 57 (2017) 46–59

Contents lists available at ScienceDirect

Signal Processing: Image Communication

journal homepage: www.elsevier.com/locate/image

A secure image sharing scheme based on SVD and Fractional Fourier Transform

Priyanka Singh*, Balasubramanian Raman, Manoj Misra

Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, Roorkee, Uttarakhand, India

ARTICLE INFO

Keywords:
Shamir secret sharing
Ownership verification
SVD
Fractional Fourier Transform

ABSTRACT

Outsourcing multimedia contents to cloud servers without obscuring may lead to an increase in security breaches that might discourage the end users from exploiting the multiple facilities provided by the cloud-based architecture. To secure the content and still be capable enough to provide the cloud services, many homomorphic encryption based schemes are being proposed in the literature. In this article, secured image outsourcing and ownership verification service in a cloud environment on the basis of singular value decomposition (SVD) and Fractional Fourier Transform (FrFT) has been proposed. It disseminates the image information via Shamir secret sharing scheme to create multiple obfuscated shares that reveal no information about the image. To assert the ownership in the encrypted domain at the receiver end, an owner specific information is embedded into some of the shares based on the secret keys. The secret information can be extracted either directly from the cloud servers or obtained after recovery of the cover media. Different attack scenarios have been analyzed considering the possibilities of the attacks that may be attempted by intruders once the information is outsourced to the cloud servers. The proposed scheme was found to be robust against various attacks, hence proving its efficacy.

1. Introduction

An increase in security and privacy breaches of multimedia data residing over the cloud-based architecture is urging researchers to investigate into new protocols and techniques that can secure the content. Hence, secure signal processing has become a very active research area. Efforts are being made to provide the same cloud services but keeping the data secure and less vulnerable to security breaches. Towards this end, many encryption schemes may be thought of as the solution of obscuring the content before outsourcing at remotely located cloud data centers. However, the limitations prevalent in these encryption schemes might not support facilitating the services on encrypted content and hence, utilization of these services becomes very challenging in encrypted domain. For decades watermarking has served as an efficient solution for protecting the multimedia content in plaintext domain [1–7]. But to do so in encrypted domain addressing the challenges of processing the encrypted content and providing a prototypical model to assert rightful ownership of encrypted content would be very beneficial. It will serve as a promising solution for scenarios where some sensitive information like a person's credentials, his medical reports, etc need to be transmitted over cloud-based paradigm without any leakage of information if any interception occurs in between.

To support different applications via secure signal processing, newer versions of transformations suited for encrypted domain processing have been proposed in the literature. Suitability of discrete Fourier transform (DFT), fast Fourier transform (FFT) and discrete cosine transform (DCT) was studied by Bianchi et al. and new variants were proposed for encrypted data [8,9]. Zheng et al. focused on transforming discrete wavelet transform (DWT) to encrypted domain and thus, reducing the data expansion persisting due to this transformation [10]. Other privacy preserving applications like fingerprint recognition [11], secure electrocardiogram (ECG) classification [12], composite signal representation [13], scale-invariant feature transform (SIFT) [14] based image feature extraction, authentication via encrypted biometrics [15], privacy-preserving face recognition [16] etc. have been proposed in the literature.

Realizing the potential of watermarking in encrypted domain to address the security issues, some works have been proposed in the literature as solutions to varied situations. A buyer-seller watermarking protocol guaranteeing the independency and confidentiality of information among buyer seller has been proposed in the literature [17]. An encrypted fingerprint logo of the buyer was embedded into the publicly encrypted information sold by the seller. Thus, the seller could

* Corresponding author.
E-mail address: priyankiitr@iitr.ac.in (P. Singh).

http://dx.doi.org/10.1016/j.image.2017.04.012
Received 3 December 2016; Received in revised form 25 April 2017; Accepted 27 April 2017
Available online 10 May 2017
0923-5965/

not get hold of the watermarked image of the buyer and buyer could not know about the original image version. A scheme to address the issue of rightful distributor in a multilevel network distribution and thus tracing the traitor if any dispute arises has been proposed in [18]. It was specifically meant for compressed and encrypted JPEG2000 content distribution.

Another joint encryption and watermarking scheme for protection of medical images has been proposed in [21]. It was aimed at maintaining the integrity of image in the encrypted domain based on stream cipher and block cipher algorithms. Although in the initial protection phase watermarking and encryption were jointly conducted, the decryption and watermark extraction could be done independently at verification stage. Integrating discrete wavelet transform and discrete cosine transform in encrypted domain for proposing a robust watermarking scheme was presented by Guo et al. [20]. Encrypting the content and thereafter compressing the least significant bits of encrypted image to hide additional information was proposed in [19]. The scheme ensured separability of secret information extraction or recovery of the original media depending on the secret keys possessed by the entity. It eradicated the flaws existing in the pipeline system where functionality of one depended on the other. Additional feature of content recovery with a new variant of visible watermarking was also explored in [22]. Reducing computational complexity and data expansion problems persisting in homomorphic encryption schemes and partial encryption schemes were proposed in [23,24]. Some regions were encrypted while others were kept in plaintext domain to embed the secret information. However, the security of plaintext regions remained vulnerable. Chinese remainder theorem (CRT) based secret sharing schemes have been proposed by Mignotte and Asmuth [25,26]. Shares are obtained based on the congruence equations and the secret can be recovered by solving the system of congruencies to get the unique solution. However, CRT based encryption schemes have been proven vulnerable to chosen plaintext attack [27].

In this article, a fully secured SVD and FrFT based image outsourcing and ownership verification service in cloud has been proposed. The scheme is based on distributing the sensitive cover media information into multiple obfuscated shares. These shares obtained via Shamir secret sharing scheme are information theoretically secure and reveals no information about the sensitive content. A owner specific secret information is embedded into some of these random looking shares by transforming using Fractional Fourier keeping the order as secret and thereafter exploiting the singular values of the transformed shares. The obtained shared are fully obscured and can be securely distributed over remotely located cloud data centers. The scheme is robust enough to handle various attack scenarios that may be possible against these encrypted shares while residing at the cloud data centers. The scheme facilitates secret information extraction either directly from the cloud data centers or after recovery of the media information at the authentic entity end possessing the secret keys. A comparison of the state-of-the-art approaches with the proposed scheme has been tabulated in Table 1. The security of the scheme relies on the value of the transform order and the chosen shares for embedding of secret information as neither the ownership information can be extracted nor the cover media can be recovered in visually recognizable quality without knowing its actual value. The proposed scheme caters the aforementioned challenges and furnishes the following goals:

- Information theoretic security: The shares residing at remotely located cloud data centers are information theoretically secure. This implies no matter how much computation power an adversary has, no information about the secret can be revealed from the shares.
- Fault tolerant: The scheme can handle the scenarios where few of the cloud data centers fully go down as the information is distributed and can be fetched from the other shares.
- Separability of secret information extraction and recovery of cover media: Depending on the secret keys, the secret information can either extracted directly from the cloud data centers or fetched after recovery of the cover media.

Table 1
Comparison of state-of-the-art methods with the proposed scheme.

Scheme	Application	Based on cryptosystem	Fault tolerant	Separability watermark of extraction & recovery of media
[17]	Buyer-seller protocol	RSA algorithm	No	No
[18]	For compressed & encrypted JPEG2000 images	Stream cipher	No	No
[19]	For data hiding or encryption	Stream cipher	No	Yes
[20]	Data embedders different from data owners	Paillier	No	Yes
[21]	For medical images	Stream cipher Block cipher	No	No
Proposed	For untrusted cloud servers	Shamir based secret sharing	Yes	Yes

Table 2
Properties of the FrFT.

Signal	FrFT
$x(t)exp(jvt)$	$exp(-jv^2(sin\alpha cos\alpha)/2 + jvcos\alpha)X_\alpha(u - vsin\alpha)$
$x(t)t$	$ucos\alpha X_\alpha(u) + jsin\alpha X_{\alpha'}(u)$
$x(t)/t$	$-jsec\alpha exp(j(u^2/2)cot\alpha)\int_{-\infty}^{u} x(z)exp(-j(z^2/2)cot\alpha)dz$
$x'(t)$	$X_{\alpha'}(u)cos\alpha + jusin\alpha X_\alpha(u)$
$\int_b^t x(t')dt'$	$sec\alpha exp(-j(u^2/2)tan\alpha)\int_b^u X_\alpha(z)exp(j(z^2/2)tan\alpha)dz$ $if\ \alpha - \pi/2\ is\ not\ a\ multiple\ of\ \pi$
$x(t-\tau)$	$exp(j(\tau^2/2)sin\alpha cos\alpha - ju\tau sin\alpha)X_\alpha(u - \tau cos\alpha)$
$x(ct)$	$\sqrt{\frac{1-jcot\alpha}{c^2-jcot\alpha}}exp(j(u^2/2))cot\alpha(1-(cos^\beta/cos^\alpha)))X_\beta(\frac{usin\alpha}{csin\alpha})$

- Robustness against different attack scenarios: The robustness of the encrypted shares was tested against different attack scenarios while residing over the cloud data centers and was found to performing satisfactorily well as evaluated by normalized cross correlation (NCC) metrics.

The rest of the paper is organized as follows: In Section 2, some preliminaries are given, Section 3 discusses the proposed approach. Experimental results along with analysis are presented in Section 4 and finally, conclusions are stated in Section 5.

2. Preliminaries

A brief overview of the concepts used in the proposed approach is given as follows:

2.1. Shamir's secret sharing

Shamir's secret sharing is a threshold based secret sharing scheme that was developed by Shamir in the year 1979 [28]. In this scheme, a secret is divided into n shares such that any k out of n shares ($k \leq n$) are sufficient to reconstruct the secret, but any combination of $k-1$ shares do not reveal any information about the secret. The shares are generated as

$$F(x) = \left(a_0 + \sum_{i=1}^{k-1} a_i x^i\right) \bmod m, \tag{1}$$

Here, m is a large prime number, a_0 is the secret, the coefficients $a_i < m$ where $a_1, a_2, \ldots a_n$ thus combine to form the shares obtained $F(x)$. The secret can be recovered by applying Lagrange interpolation using any k out of n shares. The Shamir shares thus obtained will always satisfy the homomorphism properties [29,30]. These are defined as

$$[x + a mod m]_i^m = [x]_i^m + a \bmod m, \tag{2}$$

$$[axmod m]_i^m = a\,[x]_i^m \bmod m, \tag{3}$$

where, x is the secret number, a is the constant and m is a large prime number.

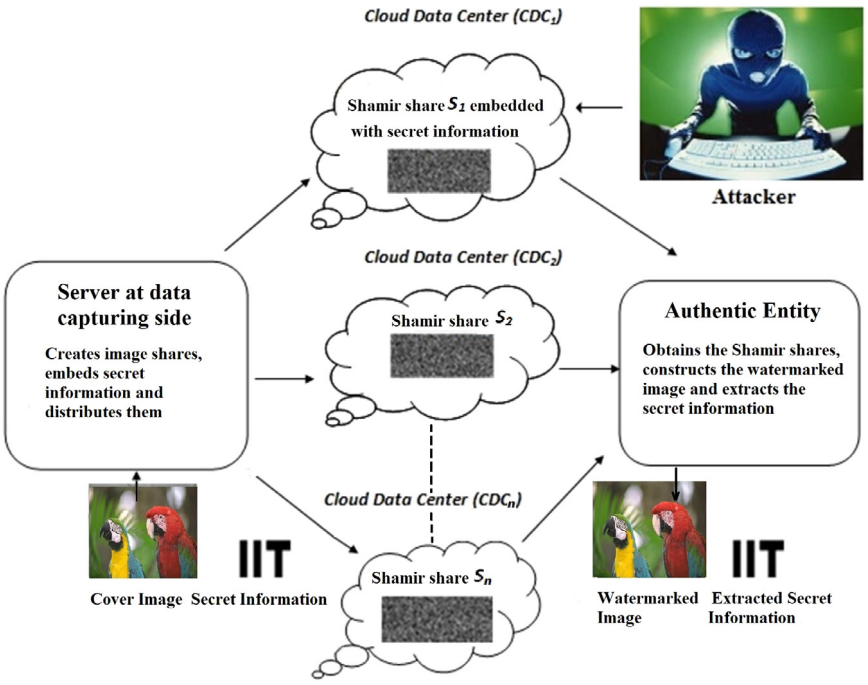

Fig. 1. Proposed cloud based architecture with some of the cloud shares (say S_1 and S_3) embedded with owner specific secret information whereas other shares (S_2, S_4, $\ldots S_n$) just composed of cover image information.

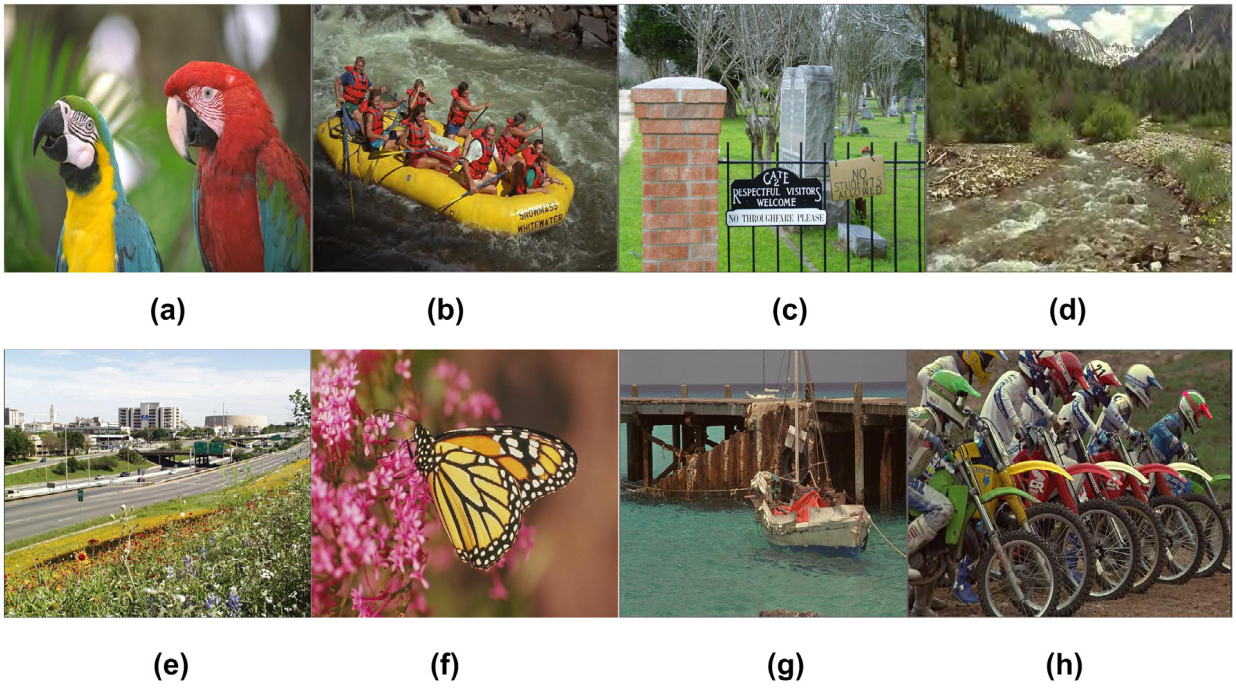

Fig. 2. Original test images.

According to these equations, performing certain operations on each share of the secret is equivalent to performing the same operations on the secret first and then dividing it into shares [28].

Fig. 3. Binary logos used as watermarks.

2.2. Fractional Fourier Transform (FrFT)

Fractional Fourier Transform (FrFT) is a generalization of Fourier transform and exists under the same conditions as the Fourier transform. It was proposed by Victor Namias in 1980 where a parameter $\alpha$was responsible for rotation in the time-frequency plane [31]. It can be mathematically defined as one dimensional function $x(t)$

$$X_\alpha(u) = F_\alpha(x(t)) = \int_{-\infty}^{\infty} x(t)K_\alpha(t,u)dt, \quad (4)$$

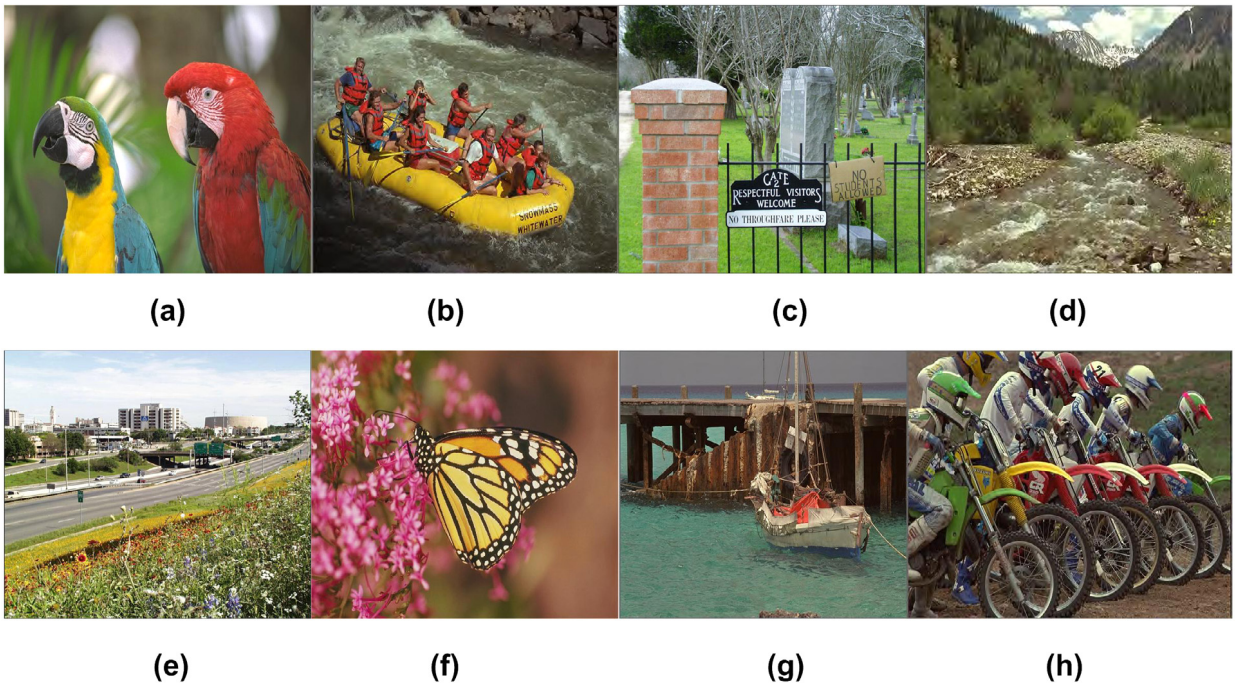

Fig. 4. Watermarked test images.

where, α is the transform order and $K_\alpha(t,u)$ is the transform kernel

$$K_\alpha(t,u)=\begin{cases}\sqrt{\dfrac{1-j\cot\alpha}{2\pi}}e^{j(\frac{u^2}{2})\cot\alpha}e^{j(\frac{t^2}{2})\cot\alpha}-ju\operatorname{csc}\alpha & \alpha\neq n\pi\\ \delta(t-u) & \alpha=2n\pi\\ \delta(t+u) & \alpha=2n\pi\pm\pi\end{cases}, \quad (5)$$

$\delta(t)$ represents the Dirac function. F_α is used throughout the paper to represent the operator associated with the FrFT. The parameter α is called order of FrFT. It has many useful properties like the separability of the transform in time-frequency domain depending on the value of α. The signal can be obtained in purely time domain if order α is 0 and purely in frequency domain if transform order (α) is $\frac{\pi}{2}$. The separability property allows the computation of higher dimensional FrFT by iteratively computing one dimensional FrFT in all the directions. Given the properties of the kernel, Eq. (4) is equal to $x(t)$ when (α) is a multiple of $\frac{\pi}{2}$ and is equal to $x(-t)$ when $(\alpha+\pi)$ is a multiple of $\frac{\pi}{2}$. Some properties of FrFT are enumerated as follows:

- Inverse FrFT can be obtained by applying $F_{-\alpha}$ to the transformed signal $(F_\alpha F_{-\alpha}=F_0)$.
- When (α) is equal to $\frac{\pi}{2}$, FrFT reduces to standard Fourier transform.
- FrFT adheres to associativity (i.e, $(F_{\alpha_3}F_{\alpha_2})F_{\alpha_1}=F_{\alpha_3}(F_{\alpha_2}F_{\alpha_1})$) and commutativity (i.e, $F_{\alpha_1}F_{\alpha_2}=F_{\alpha_2}F_{\alpha_1}$).
- FrFT is a linear operator i.e. $F_\alpha(\sum_k c_k x_k(t))=\sum_k c_k F_\alpha(x_k(t))$.
- F_0 is an identity operator, i.e. $F_0(x(t))=x(t)$. Same holds for $F_{2\pi}$.
- The effect of successive applications of FrFT of various orders is same as the sum of individual orders (e.g. $(F_\alpha F_{-\alpha}=F_{\alpha_1+\alpha_2})$.
- FrFT satisfies Parseval theorem $\langle x(t),y(t)\rangle=\langle X_\alpha(u),Y_\alpha(u)\rangle$.

FRFT is an extension of the ordinary Fourier transform and additional properties are tabulated in Table 2.

3. The proposed methodology

To facilitate security of the multimedia content residing over remotely located cloud data centers while availing facilities of cloud based architecture, the cover media information is distributed into multiple encrypted shares revealing no information. A secret owner specific information as watermark logo is embedded into some of the random shares based on a secret key. Since the shares are encrypted, they can be securely distributed over the remotely located cloud centers. Only the authentic individual possessing the secret key can obtain the watermarked image and extract information from it in the plaintext domain or directly from the cloud centers. The basic architecture of proposed scheme is depicted in Fig. 1 and the detailed phases of embedding and extraction are as follows:

Table 3
PSNR values of test images.

Image	PSNR
Parrot	63.45
Boat	65.26
Park	64.65
River Scene	61.09
City	62.88
Butterfly	63.21
Bridge	61.44
Bicycles	62.88

Table 4
Correlation coefficient of extracted logos.

Image	ρ
Parrot	1.0000
Boat	1.0000
Park	0.9998
River Scene	1.0000
City	1.0000
Butterfly	0.9999
Bridge	0.9998
Bicycles	1.0000

3.1. Distribution of cover media information into multiple obfuscated shares and embedding of owner specific information in encrypted domain

In the embedding phase, obfuscated shares are obtained via distributing information of cover media which is followed by embedding

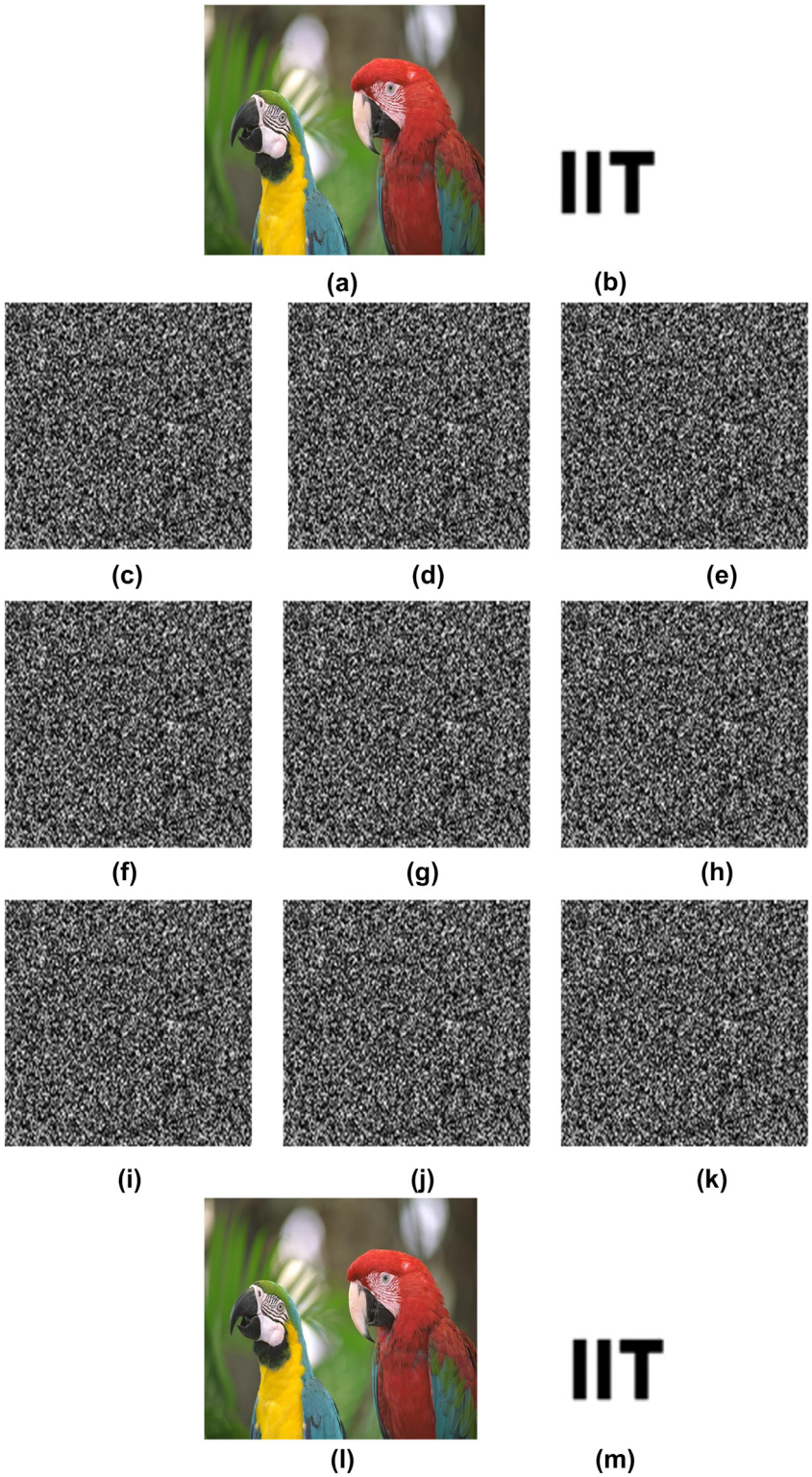

Fig. 5. Output at different stages of proposed scheme (a) Cover image (b) Secret information (c), (f), (i) Shares of cover image embedded with secret information (d), (e), (g), (h), (j), (k) Shares containing only cover image information (l) Watermarked image obtained at authentic entity after accessing all the shares (m) Extracted secret information.

of secret information into some of these shares based on a secret key. These watermarked obfuscated shares are thereafter distributed to the cloud data centers. There is no possibility of breach of security as the shares are totally random and reveal no information about the cover media. The detailed methodology is discussed as follows:

1. Generation of obfuscated shares of cover image: The information of the cover media is distributed into multiple random looking encrypted shares. The correlation existing among the neighboring pixels of the image is broken via Shamir's secret sharing scheme using Eq. (1).

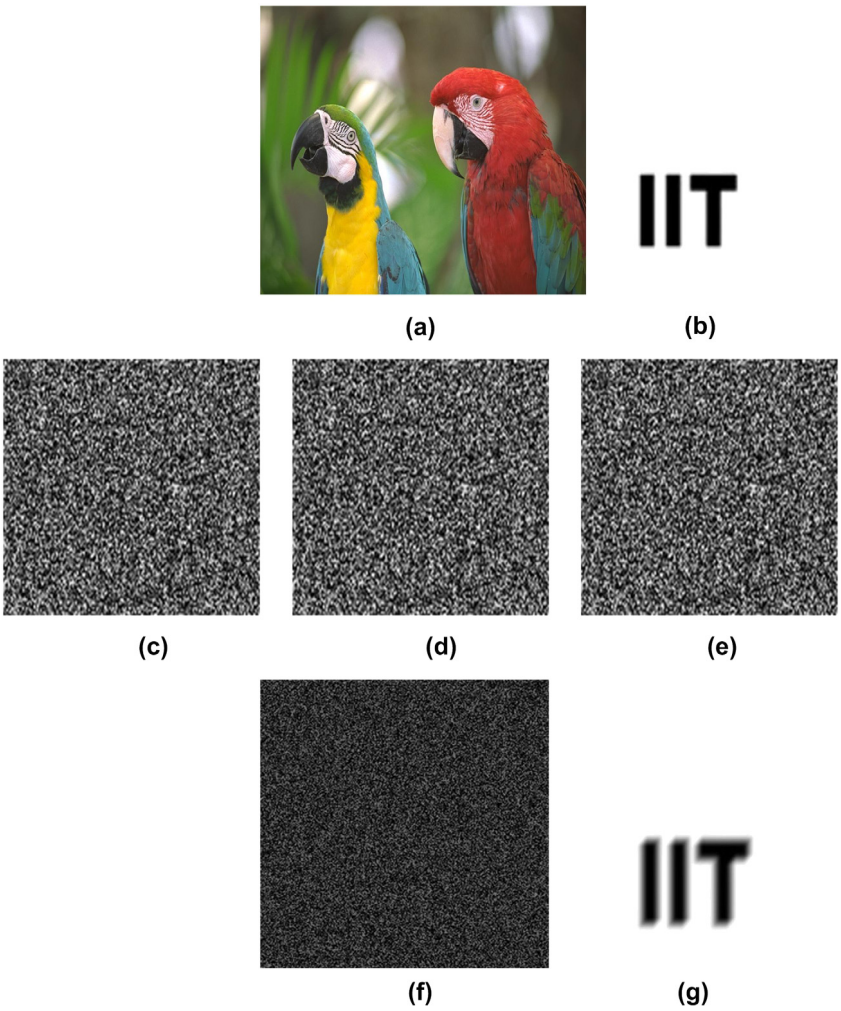

Fig. 6. Output at different stages of proposed scheme under attack scenario 1 (a) Cover image (b) Secret information (c) Attack (Motion blur) on share of cover image embedded with secret information (d), (e) Shares containing only cover image information (f) Watermarked image obtained at authentic entity after accessing k shares when more than $n-k$ shares are attacked (g) Quality of extracted secret information depends on type of attack.

Shares thus obtained follow homomorphic properties and the secret can be recovered employing Lagrange interpolation on any k out of n shares.

2. Key share selection and transformation: Based on a secret key Z, some of these obfuscated shares are selected C^Z and decomposed using the $(\alpha x, \alpha y)$ FrFT as $C^Z_{\alpha x,\alpha y}$ with αx, αy as the transform orders along x- and y-axis respectively.
3. Formation of key matrix: A key matrix is derived from the transformed cloud share $C^Z_{\alpha x,\alpha y}$ by segmenting into non-overlapping blocks $C^{Z,b}_{\alpha x,\alpha y}$ of size $p \times q$ where $p = \lfloor \frac{M}{m} \rfloor$, $q = \lfloor \frac{N}{n} \rfloor$ and $b = pq$ as total number of blocks. The singular values of the derived key matrix are modified to embed the owner information as watermark W. The detailed procedure is as follows:

   (a) For each block $C^{Z,b}_{\alpha x,\alpha y}$, compute SVD

   $$C^{Z,b}_{\alpha x,\alpha y} = U_{C^{Z,b}_{\alpha x,\alpha y}} S_{C^{Z,b}_{\alpha x,\alpha y}} V^T_{C^{Z,b}_{\alpha x,\alpha y}}. \tag{6}$$

   (b) Select the largest singular value σ_b of each block and stack it into a key matrix ζ of size $p \times q$

   $$\zeta = \begin{bmatrix} \sigma_1 & \sigma_2 & \sigma_3 & \cdots & \sigma_q \\ \sigma_{q+1} & \sigma_{q+2} & \sigma_{q+3} & \cdots & \sigma_{2q} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_{p(q+1)} & \sigma_{p(q+2)} & \sigma_{p(q+3)} & \cdots & \sigma_{pq} \end{bmatrix}. \tag{7}$$

4. Compute SVD of the obtained key matrix ζ

   $$\zeta = U_\zeta S_\zeta V^T_\zeta. \tag{8}$$

5. Perform SVD on the grayscale watermark W

   $$W = U_W S_W V^T_W. \tag{9}$$

6. Obtain the modified singular values of the key matrix

   $$S'_\zeta = S_\zeta + \alpha S_W, \tag{10}$$

   where, α gives the watermark strength.
7. Perform inverse SVD to reconstruct the modified key matrix ζ'

   $$\zeta' = U_\zeta S_{\zeta'} V^T_\zeta. \tag{11}$$

8. Replace the watermark embedded singular values into their corresponding block positions and compute inverse SVD to obtain the embedded blocks $C^{Z',b}_{\alpha x,\alpha y}$.
9. Perform inverse $(\alpha x, \alpha y)$ FrFT after replacing the modified blocks in their corresponding positions to obtain the watermarked cloud share $\widetilde{C^Z}$.

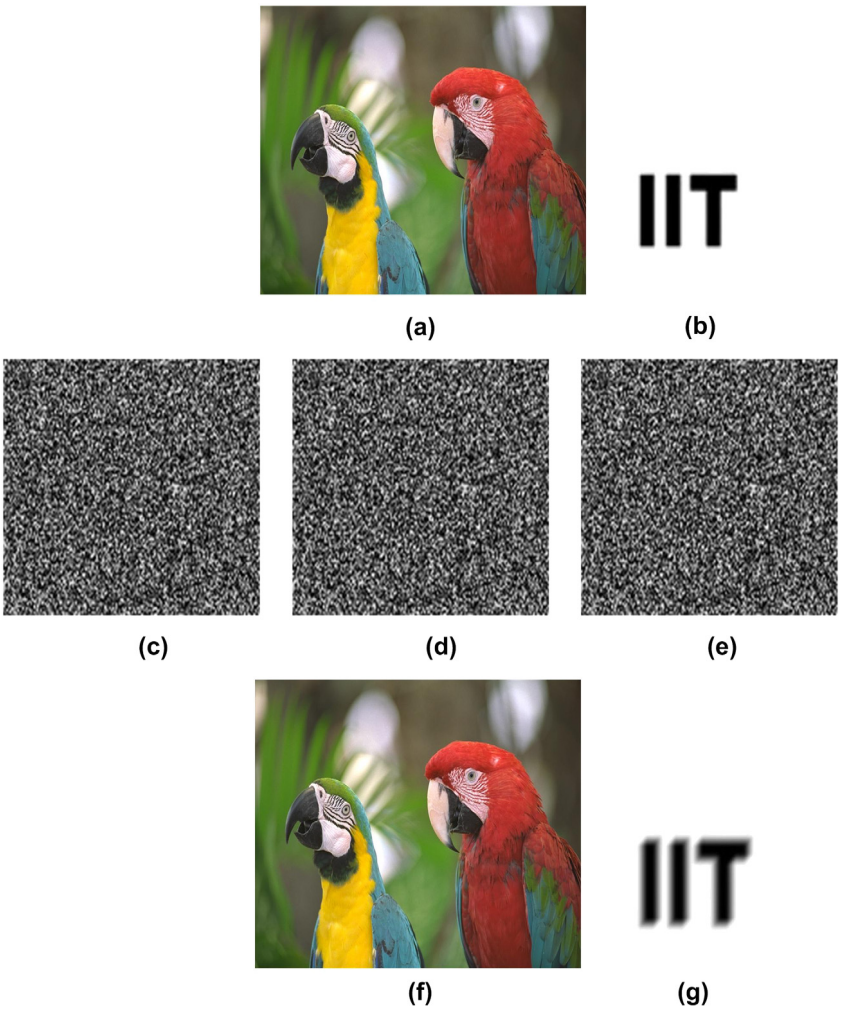

Fig. 7. Output at different stages of proposed scheme under attack scenario 2 (a) Cover image (b) Secret information (c) Attack (Motion blur) on share of cover image embedded with secret information (d), (e) Shares containing only cover image information (f) Watermarked image obtained at authentic entity after accessing k shares when less than $n-k$ shares are attacked (g) Quality of extracted secret information depends on type of attack.

3.2. Recovery of watermarked media via accessing cloud data centers and extraction of owner specific information for rightful ownership verification

The proposed scheme facilitates separability of secret information extraction for rightful ownership and recovery of the cover media at the authentic entity end possessing the secret keys. The secret information can be either extracted from the cloud data centers or obtained from the recovered watermarked media at the authentic entity.

3.2.1. Extraction of secret information from watermarked media for ownership verification

The watermarked media is obtained at the authentic entity possessing the secret keys by accessing the cloud data centers and combining the Shamir shares using Lagrange's interpolation. The obtained watermarked media may be attacked by intruders once it is reconstructed. The extraction of secret information considering the possibility of attacks is detailed as follows:

1. Reconstruction of watermarked media: The watermarked media is reconstructed at the authentic entity possessing the secret keys by combining cloud shares, in which the secret information is embedded with the other cloud shares based on Shamir secret sharing (SSS) using the Lagrange's interpolation

$$\widetilde{CW} = SSS(\widetilde{C}^Z, C^Z), \tag{12}$$

where, *SSS* is the function that combines the cloud shares using the Shamir secret sharing.

Once the watermarked media is obtained at the authentic entity, it may be attacked by the intruders which will affect the extraction of the secret information from it.

2. Generation of obfuscated shares of attacked watermarked media: Based on SSS, the attacked watermarked image $\widetilde{CW}^*$ obtained at the authentic entity is splitted into obfuscated shares.
3. Extraction of secret information from obfuscated shares of attacked watermarked media: Based on secret keys, the obfuscated shares are selected to extract the secret information from them to prove the rightful owner. The details are as follows:

   (a) Select some of the cloud shares $\widetilde{CW}^{*Z}$ based on a secret key Z and decompose it using the $(\alpha x, \alpha y)$ FrFT as $\widetilde{CW}^{*Z}_{\alpha x,\alpha y}$ with αx, αy as the transform order along x and y-axis respectively.

   (b) Formation of key matrix: Derive the key matrix from the transformed cloud share $\widetilde{CW}^{*Z}_{\alpha x,\alpha y}$ by segmenting it into non-overlapping blocks $\widetilde{CW}^{*Z,b}_{\alpha x,\alpha y}$ of same size as at the time of embedding and fetching its largest singular value $\widetilde{\sigma}_b$ to form the key matrix $\widetilde{\zeta}$

      (i) For each block $\widetilde{CW}^{*Z}_{\alpha x,\alpha y}$, compute SVD

$$\widetilde{CW}^{*Z}_{\alpha x,\alpha y} = U_{\widetilde{CW}^{*Z}_{\alpha x,\alpha y}} S_{\widetilde{CW}^{*Z}_{\alpha x,\alpha y}} V^T_{\widetilde{CW}^{*Z}_{\alpha x,\alpha y}}. \tag{13}$$

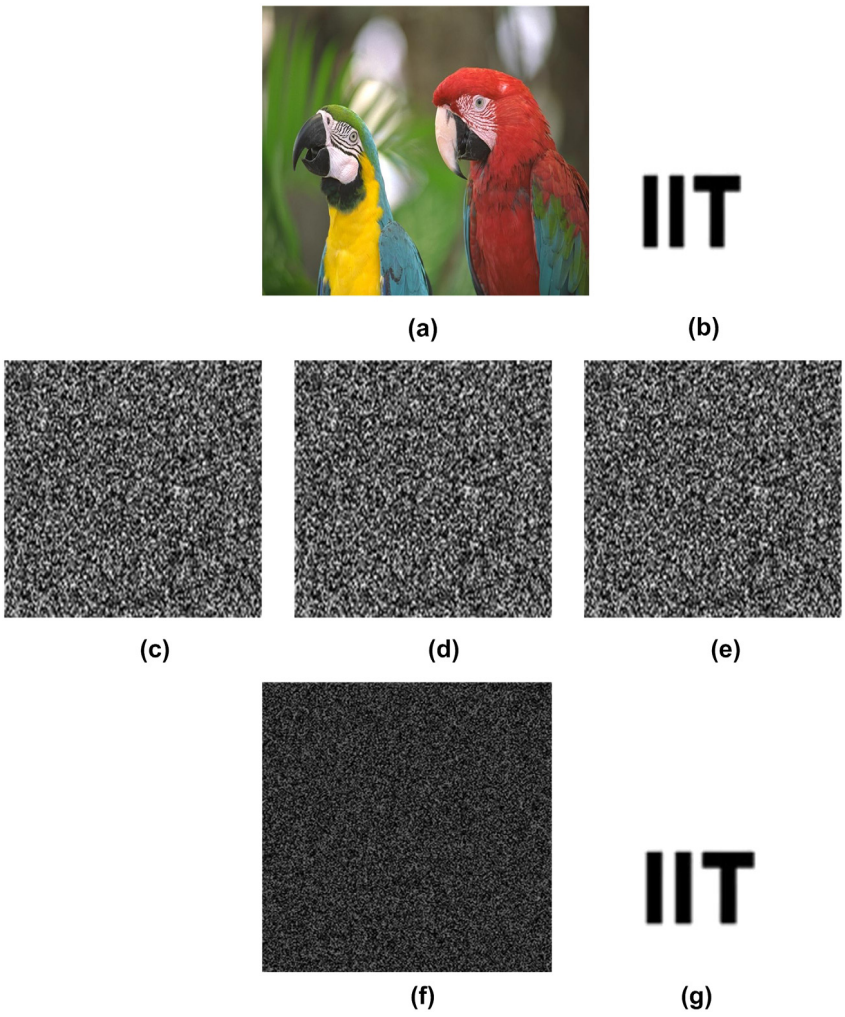

Fig. 8. Output at different stages of proposed scheme under attack scenario 3 (a) Cover image (b) Secret information (c) Share of cover image embedded with secret information (d), (e) Attack on shares containing only cover image information (f) Watermarked image obtained at authentic entity after accessing k shares when more than $n-k$ shares are attacked (g) No affect on quality of extracted secret information.

(ii) Select the largest singular value $\widetilde{\sigma}_b$ of each block and stack it into an key matrix $\widetilde{\zeta}$ of size $p \times q$

$$\widetilde{\zeta} = \begin{bmatrix} \widetilde{\sigma}_1 & \widetilde{\sigma}_2 & \widetilde{\sigma}_3 & \cdots & \widetilde{\sigma}_q \\ \widetilde{\sigma}_{q+1} & \widetilde{\sigma}_{q+2} & \widetilde{\sigma}_{q+3} & \cdots & \widetilde{\sigma}_{2q} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \widetilde{\sigma}_{p(q+1)} & \widetilde{\sigma}_{p(q+2)} & \widetilde{\sigma}_{p(q+3)} & \cdots & \widetilde{\sigma}_{pq} \end{bmatrix}. \tag{14}$$

(c) Compute SVD of the obtained key matrix $\widetilde{\zeta}$

$$\widetilde{\zeta} = U_{\widetilde{\zeta}} S_{\widetilde{\zeta}} V_{\widetilde{\zeta}}^T. \tag{15}$$

(d) Extract the singular values of the grayscale watermark W

$$S_{W^{Ext}} = \frac{S_{\widetilde{\zeta}} - S_{\zeta}}{\alpha}, \tag{16}$$

where, α represents the watermark strength.

(e) Obtain the extracted watermark

$$W^{Ext} = U_W S_{W^{Ext}} V_W^T. \tag{17}$$

3.2.2. Extraction of secret information directly from the cloud data centers for ownership verification

The information of the cover media is distributed into multiple encrypted shares prior to outsourcing at the cloud centers. Though rendering the information into encrypted form removes the possibility of information leakage at the cloud centers but still the intruder can attack the encrypted shares without knowing its content. If the cloud centers holding the secret information embedded shares are attacked, it will affect the rightful ownership verification as the extracted secret information will get affected. But if the other cloud data centers are attacked, it will not make any difference on the ownership verification process. The details of secret information extraction from the attacked embedded shares is as follows:

(a) Decompose the cloud share $\widetilde{CW}^{*Z}$ using the $(\alpha x, \alpha y)$ FrFT as $\widetilde{CW}^{*Z}_{\alpha x,\alpha y}$ with αx, αy as the transform order along x and y-axis respectively.

(b) Derive the key matrix from the transformed cloud share $\widetilde{CW}^{*Z}_{\alpha x,\alpha y}$ by segmenting it into non-overlapping blocks $\widetilde{CW}^{*Z,b}_{\alpha x,\alpha y}$ and fetching its largest singular value $\widetilde{\sigma}_b$ to form the key matrix $\widetilde{\zeta}$ as follows:

(i) For each block $\widetilde{CW}^{*Z}_{\alpha x,\alpha y}$, compute SVD

$$\widetilde{CW}^{*Z}_{\alpha x,\alpha y} = U_{\widetilde{CW}^{*Z}_{\alpha x,\alpha y}} S_{\widetilde{CW}^{*Z}_{\alpha x,\alpha y}} V^T_{\widetilde{CW}^{*Z}_{\alpha x,\alpha y}}. \tag{18}$$

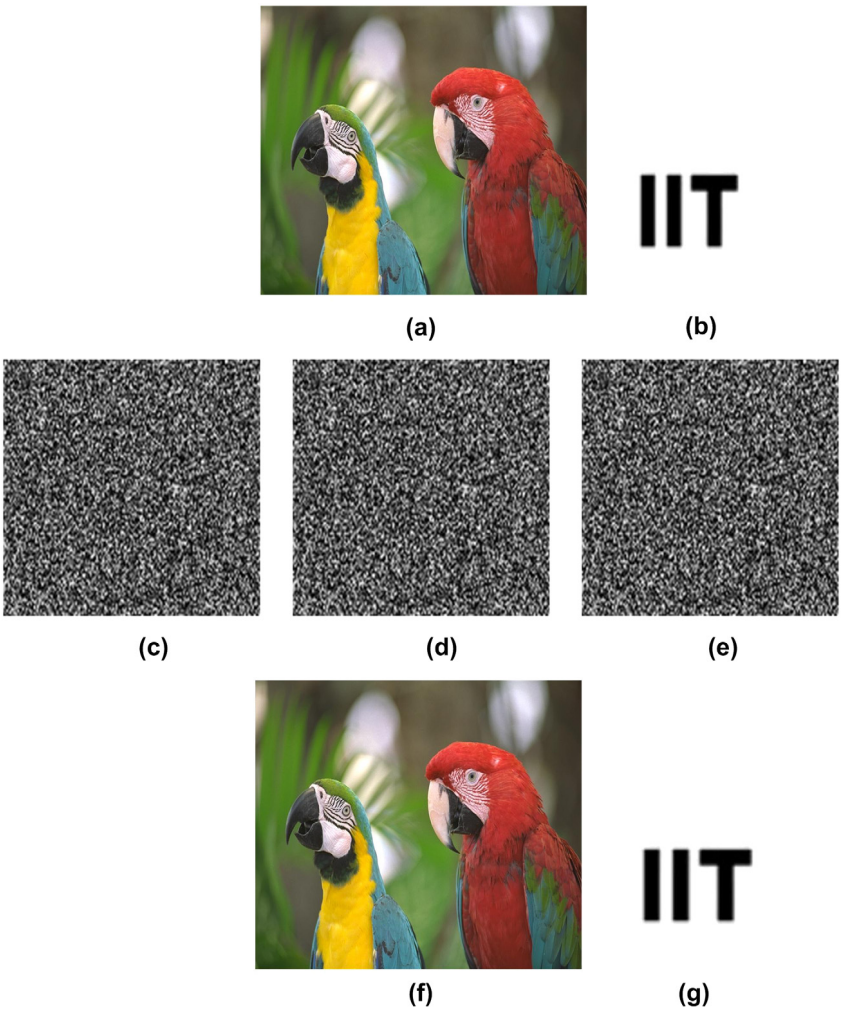

Fig. 9. Output at different stages of proposed scheme under attack scenario 4 (a) Cover image (b) Secret information (c) Share of cover image embedded with secret information (d), (e) Attack on shares containing only cover image information (f) Watermarked image obtained at authentic entity after accessing after accessing k shares when less than $n-k$ shares are attacked (g) No affect on quality of extracted secret information.

(ii) Select the largest singular value $\widetilde{\sigma}_b$ of each block and stack it into an key matrix $\widetilde{\zeta}$ of size $p \times q$

$$\widetilde{\zeta} = \begin{bmatrix} \widetilde{\sigma}_1 & \widetilde{\sigma}_2 & \widetilde{\sigma}_3 & \cdots & \widetilde{\sigma}_q \\ \widetilde{\sigma}_{q+1} & \widetilde{\sigma}_{q+2} & \widetilde{\sigma}_{q+3} & \cdots & \widetilde{\sigma}_{2q} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \widetilde{\sigma}_{p(q+1)} & \widetilde{\sigma}_{p(q+2)} & \widetilde{\sigma}_{p(q+3)} & \cdots & \widetilde{\sigma}_{pq} \end{bmatrix}. \tag{19}$$

(c) Compute SVD of the obtained key matrix $\widetilde{\zeta}$

$$\widetilde{\zeta} = U_{\widetilde{\zeta}} S_{\widetilde{\zeta}} V_{\widetilde{\zeta}}^T. \tag{20}$$

(d) Extract the singular values of the grayscale watermark W

$$S_{W^{Ext}} = \frac{S_{\widetilde{\zeta}} - S_{\zeta}}{\alpha}, \tag{21}$$

where, α represents the watermark strength.

(e) Obtain the extracted watermark

$$W^{Ext} = U_W S_{W^{Ext}} V_W^T. \tag{22}$$

4. Experimental results and discussion

The wide attacking surface of the cloud-based architecture demands for secure approaches that can facilitate usage of cloud infrastructure and storage capacities but in a secured way. The proposed scheme based on Shamir's secret sharing furnishes one such approach where the information of the cover media is distributed into multiple encrypted shares that are information theoretically secure. It implies that no matter how much power an attacker possesses, no information could be revealed from the shares.

To facilitate ownership verification of the encrypted media, a secret owner specific information is embedded into some of these encrypted shares based on a secret key. The information embedded shares are also obtained in encrypted form itself and reveal no information. Hence, they can be outsourced to remotely distributed cloud data centers without any vulnerability to security breaches. Experiments have been simulated with MATLAB as the implementation tool with a wide variety of standard test cover color images of size 512×512. Some are presented in Fig. 2 namely Parrot, Boat, Park, River Scene, City, Butterfly, Bridge and Bicycles. Owner information were taken to be sets of grayscale logos of size 128×128 in the experiments. Some of these logos are depicted in Fig. 3 namely IT, IIT, Circles, IEEE and PS.

The copyright logos were embedded into some of these obfuscated shares of the various test cover images like logo circles is embedded into Parrot and Boat, logo PS in Bicycles and River Scene, logo IT in City and Butterfly, logo IIT in Bridge and IEEE logo in Park test images. The watermarked image obtained at the authentic entity end via Shamir reconstruction after accessing the cloud data center shares

Fig. 10. Results of various attacks (i) Salt & Pepper noise addition attack (ii) Speckle noise addition attack (iii) Disk filtering attack (iv) Weiner filtering attack where (a), (c) Watermarked test images (b), (d) Extracted logos.

was visually imperceptible with respect to the original cover media as shown in Fig. 4. The visual quality was evaluated based on peak signal to noise ratio (PSNR) with values tabulated in Table 3. The proposed scheme facilitates separability of secret information extraction from the recovery of the cover media. The secret information can be either directly extracted from the cloud data centers or obtained after recovery of the cover media at the authentic entity possessing the secret keys. The extracted watermark logos are evaluated based on NCC values tabulated in Table 4. The strength factor α used in the experiments was 0.032.

The output obtained at different stages of the proposed scheme has been depicted in Fig. 5 for one of the test cover images. The scheme distributes (a) the information of the cover media into multiple random looking shares (c) to (k) that are information theoretically secure. Based on the secret keys, (b) the owner specific information is embedded into some of the obfuscated shares (say share (c)) which remain encrypted and can be sent securely to the distributed cloud data centers. At the authentic entity end, the watermarked image can be obtained back as shown in (l) and secret information can be extracted from it as depicted in (m).

To investigate the efficacy of the proposed watermarking scheme in the encrypted domain, a series of experiments were conducted considering different scenarios. Although the proposed scheme reduces the vulnerability of the encrypted shares towards information leakage at the cloud data centers, the shares may still be attacked by intruders without knowing their actual content. The attacker may attack the cloud data center holding the share with embedded secret information or the other data centers. The effect of the attacks considering the aforementioned scenarios have been depicted in Figs. 6–9 respectively. The extraction of the secret information would get affected if the attack is done on the cloud data center containing the embedded share as shown in Figs. 6 and 7 for one of the attacks (Motion Blur). Otherwise, if the attacker tampers the other data centers, it will not affect the extraction of the secret information and its visual quality as shown in Figs. 8 and 9. The recovered image will only get affected when more than n-k shares are attacked simultaneously.

The robustness of the proposed scheme have been tested against different attack scenarios like distortions introduced by different noises as salt & pepper noise, speckle noise, Gaussian noise etc, filtering manipulations such as disk filter, Weiner filtering, Laplacian filter, average filtering, Sobel filter, log filter, median filtering, Gaussian filter, standard deviation filter, etc. Other possible alterations such as histogram equalization, resizing, unsharp masking, motion blur, etc have

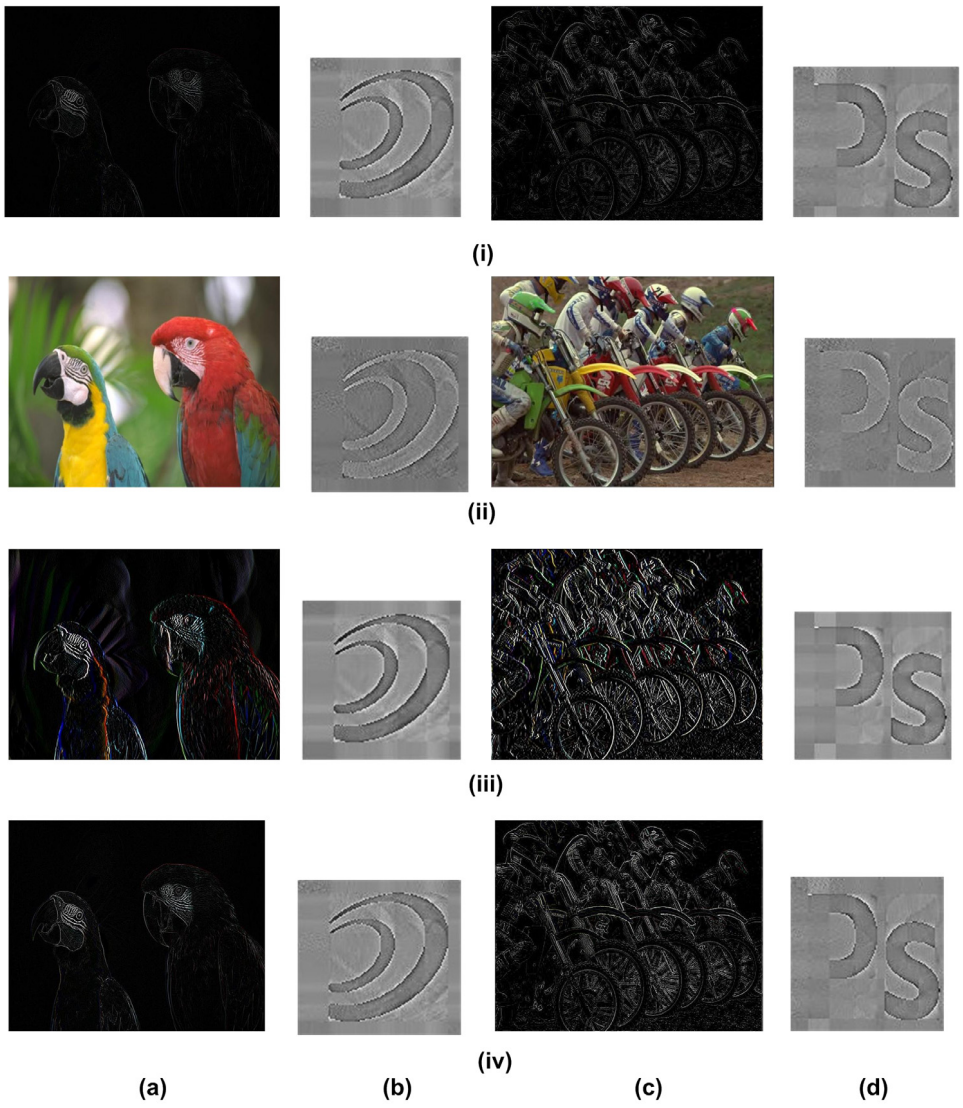

Fig. 11. Results of various attacks (i) Laplacian filtering attack (ii) Average filtering attack (iii) Sobel filtering attack (iv) Log filtering attack where (a), (c) Watermarked test images (b), (d) Extracted logos.

also been tested with. The secret information (watermark logos) could be either extracted directly from the cloud data centers or extracted from the watermarked media once it is obtained at the authentic entity. Results for two of the test images i.e Parrot and Bicycles have been shown for further analysis considering the Circles and PS as the secret information. For visually assessing the effects of the attacks, some of the attacks are depicted in Figs. 10–13 with quantitative evaluation based on the correlation values tabulated in Tables 5 and 6. The details of the different attacks are described as follows:

As first attack, distortion was introduced by salt & pepper noise to the watermarked image reconstructed via encrypted shares as well as to the individual cloud data shares with 0.09 noise density. The extracted watermark was visually recognizable as depicted in Fig. 10(i). Other kind of noises were also tested like the speckle noise with 0.07 noise density and Gaussian noise with 0.06 noise density. The extracted watermarks were identified well as shown in Fig. 10(ii).

Various kind of filters with varying mask sizes were tested with the reconstructed watermarked image as well as the individual cloud data shares. In particular, median filter with 15×15 mask, Sobel filter, Weiner filter with 15×15 mask, Gaussian filter, Laplacian filter, average filter, standard deviation filter, etc were applied with results depicted in Figs. 10–12. Disk filter with radius of 15 within square matrix of size 23 was applied to the reconstructed watermarked image as well as to the individual cloud data centers. Identifiable watermarks were extracted as depicted in Fig. 10(iii). Histogram equalization was attempted as the attack scenario to alter the contrast of the watermarked image as well as the encrypted cloud shares. Visually recognizable watermarks were extracted as represented in Fig. 12(iii). Resizing of the reconstructed watermarked image was done from original size of 512×512 to 256×256 and back to 512×512. The same was tested for the individual encrypted shares with extracted watermarks represented in Fig. 12(iv). Unsharp masking was applied as another attack to the watermarked image obtained at the authentic entity after accessing all the cloud shares. A visual recognizable watermark is extracted from the distorted watermarked image due to the effect of the attack as depicted in Fig. 13(i). Motion blur was also tested as an attack on the watermarked image obtained at the authentic entity as well as the individual cloud data centers. The camera was moved by 50 degrees in counterclockwise direction with linear motion of 24 pixels. The extracted watermark is depicted in Fig. 13(ii). JPEG compression with 80:1 compressed watermarked image as well as the cloud data shares was tested for robustness of the scheme against image compression attack with results tabulated in Tables 5 and 6 respectively.

Fig. 12. Results of various attacks (i) Median filtering attack (ii) Gaussian filtering attack (iii) Histogram equalization attack (iv) Resizing attack where (a), (c) Watermarked test images (b), (d) Extracted logos.

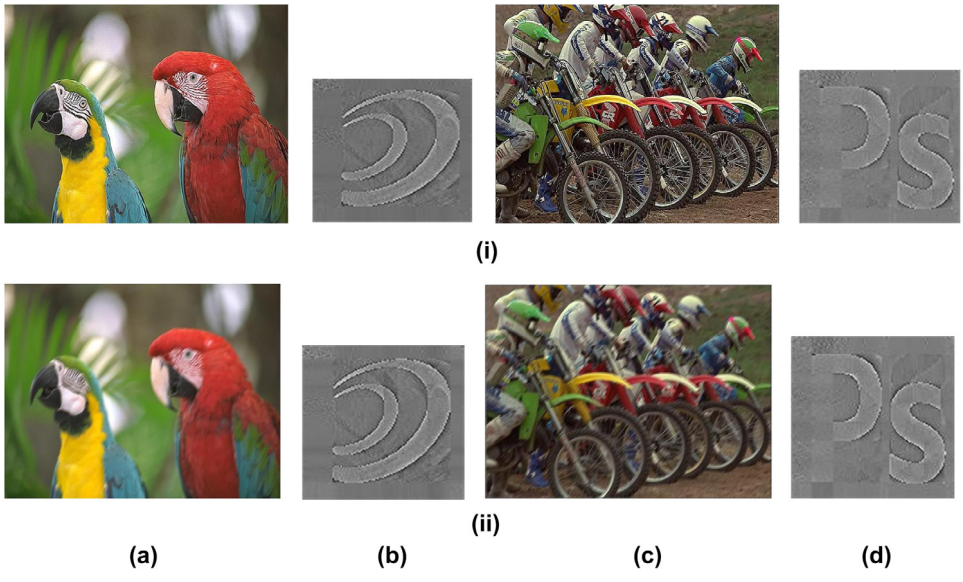

Fig. 13. Results of various attacks (i) Unsharp masking attack (ii) Motion blur attack where (a), (c) Watermarked test images (b), (d) Extracted logos.

Table 5
Correlation coefficient of watermark extracted directly from the cloud data centers after attacks.

Attacks	Parrot	Bicycles
With watermarking(no attack)	1.0000	1.0000
Histogram equalization	0.7564	0.7684
Gaussian blur	0.6413	0.6517
Speckle noise	0.7528	0.7483
Salt & pepper noise (50%)	0.7319	0.7309
Resizing (512 → 256 → 512)	0.6387	0.6484
Median filtering	0.6384	0.6465
Average filter	0.6422	0.6422
Motion blur	0.6482	0.6587
Unsharp masking	0.6542	0.6601
Laplacian filter	0.6464	0.6616
Log filter	0.6485	0.6514
Sobel filter	0.6550	0.6705
Standard deviation filter	0.6617	0.6515
Weiner filter	0.6433	0.6534
Disk filter	0.6479	0.6586
Gaussian noise	0.7556	0.7532
JPEG	0.6560	0.6615

Table 6
Correlation coefficient of watermark extracted from attacked watermarked image obtained at the authentic entity.

Attacks	Parrot	Bicycles
With watermarking(no attack)	1.0000	1.0000
Histogram equalization	0.6415	0.6570
Gaussian blur	0.6851	0.6360
Speckle noise	0.6589	0.6454
Salt & pepper noise (50%)	0.6517	0.6607
Resizing (512 → 256 → 512)	0.6568	0.6461
Median filtering	0.6543	0.6592
Average filter	0.6620	0.6429
Motion blur	0.6477	0.6766
Unsharp masking	0.6592	0.6425
Laplacian filter	0.6562	0.6957
Log filter	0.6430	0.6535
Sobel filter	0.6983	0.6728
Standard deviation filter	0.6537	0.6489
Weiner filter	0.7040	0.7285
Disk filter	0.6472	0.6476
Gaussian noise	0.6587	0.6426
JPEG	0.65208	0.6550

5. Conclusion

For the purpose of decreasing the susceptibility of sensitive multimedia information residing over distributed cloud data centers managed by third party servers, a secure SVD-FrFT based watermarking scheme for encrypted domain has been proposed in this paper. The sensitive information was secured via distributing its content into multiple random looking Shamir shares. A secret information was embedded into some of its random looking shares to prove the rightful ownership of the content on the receiver end. The robustness of the scheme was tested against different attacks possible by the intruders once the information is outsourced at the cloud data centers. The scheme could even tolerate the scenarios in which some of the cloud servers fully go down and was found to be performing satisfactorily well against different attack scenarios in encrypted domain itself. The recovery of the media also remained unaffected unless more than $n - k$ shares were attacked simultaneously.

References

[1] G. Bhatnagar, B. Raman, A new robust reference watermarking scheme based on dwt-svd, Comput. Stand. Interfaces 31 (5) (2009) 1002–1013. http://dx.doi.org/10.1016/j.csi.2008.09.031. (Specification, Standards and Information Management for Distributed Systems <http://www.sciencedirect.com/science/article/pii/S0920548908001499>.

[2] S. Rawat, B. Raman, A chaotic system based fragile watermarking scheme for image tamper detection, AEU - Int. J. Electron. Commun. 65 (10) (2011) 840–847. http://dx.doi.org/10.1016/j.aeue.2011.01.016. <http://www.sciencedirect.com/science/article/pii/S1434841111000227)>.

[3] C. Qin, H. Wang, X. Zhang, X. Sun, Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode, Inf. Sci. 373 (2016) 233–250. http://dx.doi.org/10.1016/j.ins.2016.09.001. <http://www.sciencedirect.com/science/article/pii/S0020025516307150>.

[4] G. Bhatnagar, Q.J. Wu, B. Raman, Discrete fractional wavelet transform and its application to multiple encryption, Inf. Sci. 223 (2013) 297–316. http://dx.doi.org/10.1016/j.ins.2012.09.053. <http://www.sciencedirect.com/science/article/pii/S0020025512006469>.

[5] A.M. Buhari, H.-C. Ling, V.M. Baskaran, K. Wong, Fast watermarking scheme for real-time spatial scalable video coding, Signal Process.: Image Commun. 47 (2016) 86–95. http://dx.doi.org/10.1016/j.image.2016.06.003. <http://www.sciencedirect.com/science/article/pii/S0923596516300893>.

[6] D. Bouslimi, G. Coatrieux, A crypto-watermarking system for ensuring reliability control and traceability of medical images, Signal Process.: Image Commun. 47 (2016) 160–169. http://dx.doi.org/10.1016/j.image.2016.05.021. <http://www.sciencedirect.com/science/article/pii/S0923596516300868>.

[7] Z. Shao, Y. Shang, R. Zeng, H. Shu, G. Coatrieux, J. Wu, Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography, Signal Process.: Image Commun. 48 (2016) 12–21. http://dx.doi.org/10.1016/j.image.2016.09.001. <http://www.sciencedirect.com/science/article/pii/S0923596516301175>.

[8] T. Bianchi, A. Piva, M. Barni, Encrypted domain dct based on homomorphic cryptosystems, EURASIP J. Inf. Secur. 2009 (1–1) (2009) 1–12. http://dx.doi.org/10.1155/2009/716357. <http://dx.doi.org/10.1155/2009/716357>.

[9] T. Bianchi, A. Piva, M. Barni, On the implementation of the discrete fourier transform in the encrypted domain, IEEE Trans. Inf. Forensics Secur. 4 (1) (2009) 86–97. http://dx.doi.org/10.1109/TIFS.2008.2011087.

[10] P. Zheng, J. Huang, Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain, Trans. Img. Proc. 22 (6) (2013) 2455–2468. http://dx.doi.org/10.1109/TIP.2013.2253474. <http://dx.doi.org/10.1109/TIP.2013.2253474>.

[11] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva, F. Scotti, A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates, in: IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), 2010, pp. 1–7. <http://dx.doi.org/10.1109/BTAS.2010.5634527>.

[12] M. Barni, P. Failla, R. Lazzeretti, A.R. Sadeghi, T. Schneider, Privacy-preserving ecg classification with branching programs and neural networks, IEEE Trans. Inf. Forensics Secur. 6 (2) (2011) 452–468. http://dx.doi.org/10.1109/TIFS.2011.2108650.

[13] T. Bianchi, A. Piva, M. Barni, Composite signal representation for fast and storage-efficient processing of encrypted signals, IEEE Trans. Inf. Forensics Secur. 5 (1) (2010) 180–187. http://dx.doi.org/10.1109/TIFS.2009.2036230.

[14] C.Y. Hsu, C.S. Lu, S.C. Pei, Image feature extraction in encrypted domain with privacy-preserving sift, IEEE Trans. Image Process. 21 (11) (2012) 4593–4607. http://dx.doi.org/10.1109/TIP.2012.2204272.

[15] P. Failla, Y. Sutcu, M. Barni, esketch: A privacy-preserving fuzzy commitment scheme for authentication using encrypted biometrics, in: Proceedings of the 12th ACM Workshop on Multimedia and Security, MM&Sec '10, ACM, New York, NY, USA, 2010, pp. 241–246. <http://dx.doi.org/10.1145/1854229.1854271http://doi.acm.org/10.1145/1854229.1854271>.

[16] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, T. Toft, Privacy-Preserving Face Recognition, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009, 235–253. http://dx.doi.org/10.1007/978-3-642-03168-7_14. <http://dx.doi.org/10.1007/978-3-642-03168-7_14>.

[17] N. Memon, P.W. Wong, A buyer-seller watermarking protocol, IEEE Trans. Image Process. 10 (4) (2001) 643–649. http://dx.doi.org/10.1109/83.913598.

[18] A.V. Subramanyam, S. Emmanuel, M.S. Kankanhalli, Robust watermarking of compressed and encrypted jpeg2000 images, IEEE Trans. Multimed. 14 (3) (2012) 703–716. http://dx.doi.org/10.1109/TMM.2011.2181342.

[19] X. Zhang, Separable reversible data hiding in encrypted image, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 826–832. http://dx.doi.org/10.1109/TIFS.2011.2176120.

[20] J. Guo, P. Zheng, J. Huang, Secure watermarking scheme against watermark attacks in the encrypted domain, J. Vis. Commun. Image Represent. 30 (2015) 125–135. http://dx.doi.org/10.1016/j.jvcir.2015.03.009. <http://www.sciencedirect.com/science/article/pii/S1047320315000590>.

[21] D. Bouslimi, G. Coatrieux, M. Cozic, C. Roux, A joint encryption/watermarking system for verifying the reliability of medical images, IEEE Trans. Inf. Technol. Biomed. 16 (5) (2012) 891–899. http://dx.doi.org/10.1109/TITB.2012.2207730.

[22] X. Zhang, Z. Wang, J. Yu, Z. Qian, Reversible visible watermark embedded in encrypted domain, in: Signal and Information Processing (ChinaSIP), 2015 IEEE China Summit and International Conference on, 2015, pp. 826–830. <http://dx.doi.org/10.1109/ChinaSIP.2015.7230520>.

[23] S. Lian, Z. Liu, Z. Ren, H. Wang, Commutative encryption and watermarking in video compression, IEEE Trans. Circuits Syst. Video Technol. 17 (6) (2007) 774–778. http://dx.doi.org/10.1109/TCSVT.2007.896635.

[24] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F.G.B. de Natale, A. Neri, A commutative digital image watermarking and encryption method in the tree structured haar transform domain, Image Commun. 26 (1) (2011) 1–12. http://dx.doi.org/10.1016/j.image.2010.11.001. <http://dx.doi.org/10.1016/j.image.2010.11.001>.

[25] M. Mignotte, How to share a secret, in: Proceedings of the 1982 Conference on Cryptography, 1983, pp. 371–375.

[26] C. Asmuth, J. Bloom, A modular approach to key safeguarding, IEEE Trans. Inf. Theory 29 (2) (1983) 208–210. http://dx.doi.org/10.1109/TIT.1983.1056651.

[27] C. Li, Y. Liu, L.Y. Zhang, K.-W. Wong, Cryptanalyzing a class of image encryption schemes based on chinese remainder theorem, Signal Process.: Image Commun. 29 (8) (2014) 914–920. http://dx.doi.org/10.1016/j.image.2014.06.011. <http://www.sciencedirect.com/science/article/pii/S0923596514001052>.

[28] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613. http://dx.doi.org/10.1145/359168.359176. <http://doi.acm.org/10.1145/359168.359176>.

[29] J. Cohen Benaloh, Secret sharing homomorphisms: Keeping shares of a secret secret, in: Proceedings on Advances in cryptology—CRYPTO '86, Springer-Verlag, London, UK, 1987, pp. 251–260. <http://dl.acm.org/citation.cfm?Id=36664.36683>.

[30] S. M. S. N. Esfahani, Y. Luo, S. c. S. Cheung, Privacy protected image denoising with secret shares, in: 2012 Proceedings of the 19th IEEE International Conference on Image Processing, 2012, pp. 253–256. <http://dx.doi.org/10.1109/ICIP.2012.6466843>.

[31] V. NAMIAS, The fractional order fourier transform and its application to quantum mechanics, IMA Journal of Applied Mathematics, 25(3), 1980, pp. 241–265. <arXiv:25/3/241.full.pdf+html>, <http://dx.doi.org/10.1093/imamat/25.3.241>. <http://imamat.oxfordjournals.org/content/25/3/241.abstract>.