Optica Applicata, Vol. XLVIII, No. 1, 2018
DOI: 10.5277/oa180103

Color image encryption using singular value decomposition in discrete cosine Stockwell transform domain

ANKITA VAISH[1*], MANOJ KUMAR[2]

[1] Banaras Hindu University, Varanasi, India

[2] Babasaheb Bhimrao Ambedkar University (A Central University),
Vidya Vihar, Lucknow, India

[*] Corresponding author: av21lko@gmail.com

In this paper, an image encryption technique using singular value decomposition (SVD) and discrete cosine Stockwell transform (DCST) is proposed. The original source image is encrypted using bands of DCST along with the SVD decomposed images. The number of bands in DCST, parameters used to mask the singular values, the way of permutation used to shuffle the values of SVD transformed images and the way of arrangement of SVD matrices are used as encryption keys. It is necessary to have correct knowledge of all the keys along with their respective values, for correct decryption of encrypted images. The robustness and the quality measurement of proposed work are analyzed by comparing it with some existing works.

Keywords: discrete cosine Stockwell transform, image encryption, singular value decomposition, mean square error, structural similarity index measurement.

1. Introduction

The advancement in digital technology gives rise to several applications in image processing. Due to security reasons, direct transmission of multimedia content over the public networks is not usually preferred. Multimedia in the form of digital images is used in several fields such as: defense, medical, artwork, *etc*. Many rigorous efforts have been made by researchers to keep the information secure from unauthorized people. First optical encryption technique is given by REFREGIER and JAVIDI [1], which uses a double random phase (DRP). After that various techniques have been proposed for secure image transmission. These techniques can be categorized based on the domain viz. techniques based on digital holography [2], Hartley transform [3–5], Arnold transform [6–8], gyrator transform [9–15], and fractional Mellin transform [16, 17]. In the current era, compressive sensing [18–20], log polar [21], quantum computation [22, 23] and fractional Fourier transform [24–31] based techniques are also being developed more frequently.

In Hartley transform domain, an image encryption technique is given by Singh and Sinha [3] using logistic map. Linfei Chen and Daomu Zhao [4] proposed an image encryption technique based on interferometer in Hartley domain. An image encryption technique using chaotic map is proposed by Zhengjun Liu *et al.* [5] which uses baker map to scramble the values of color planes.

Various color image encryption techniques have been developed using Arnold transform. Arnold transform scrambles the position of pixel values, which results in a random image. Qing Guo *et al.* [6] proposed a color image encryption technique in intensity I, hue H and saturation S color planes using Arnold and fractional random transforms; in that work I plane is secured using fractional random transforms and H and S planes are encrypted using Arnold transform. An image encryption technique using Arnold transform and discrete cosine transform is developed by Zhengjun Liu *et al.* [7]. Again, Zhengjun Liu *et al.* [8] proposed a color image encryption technique using discrete angular and Arnold transform.

Several color image encryption techniques have been given by various researchers in gyrator transform domain, viz. Singh and Sinha [9] proposed an image encryption technique using chaos. A significant amount of work has been done by Abuturab [10 –15] in gyrator transform domain: an image encoding technique using a DRP is given by Abuturab [10]. Further, Abuturab [11] has given an image encryption technique using Arnold transform. Again, a new technique based on Hartley transform in gyrator transform domain is developed by Abuturab [13]. More recently, a color image encryption technique is developed using singular value decomposition (SVD) in gyrator transform domain [15].

Some optical image encryption techniques have also been developed in fractional Mellin transform (FrMT) domain. Nanrun Zhou *et al.* [16] proposed an image encryption technique in FrMT domain. The use of the nonlinear FrMT makes this work secure against conventional encryption techniques. A novel image compression and encryption technique have been developed by Nanrun Zhou *et al.* [17] using compressive sensing in FrMT domain, in which compression and encryption are obtained simultaneously by measuring the original image using measurement matrices in two directions. The resultant image is re-encrypted using FrMT.

A few image compression and encryption techniques are also developed using compressive sensing such as a novel image compression-encryption technique developed by Nanrun Zhou *et al.* [18] using compressive sensing and hyper chaotic system. Nanrun Zhou *et al.* [19] proposed a novel hybrid compression and encryption technique using a key-controlled measurement matrix in compressive sensing. Again a new compression-encryption method using compressive sensing is proposed by Nanrun Zhou *et al.* [20], in that work the measurement matrix is constructed as a partial Hadamard matrix.

Only several of the researchers have put their efforts to develop secure image encryption techniques using a log polar transform: Lihua Gong *et al.* [21] proposed a novel image encryption method using a log polar transform with DRP encoding in fractional

Fourier transform domain, which exploits the data compression ability of the log polar transform in image encryption.

Recently, quantum images are also used in various fields of information science. The ever growing field of quantum computation and quantum computers has attracted several researchers to investigate novel quantum image encryption techniques. A new image encryption technique using quantum Fourier transform and DRP encoding is developed by YU-GUANG YANG *et al*. [22]. Further, NAN RUN ZHOU *et al*. [23] has also analyzed the security of quantum image using generalized Arnold transform and DRP encoding, where pixels are scrambled using generalized Arnold transform and gray level information encoded using DRP encoding technique.

Many color image encryption methods have been proposed using fractional Fourier transform (FrFT). FrFT is a generalized version of the traditional Fourier transform. A random FrFT is also proposed by ZHENGJUN LIU and SHUTIAN LIU [24] which is obtained by randomizing the conventional FrFT. SHUTIAN LIU *et al*. [25] proposed an encryption technique using multi-channel and multi-stage FrFT domain filtering. An iterative FrFT based image encryption technique is proposed by YAN ZHANG *et al*. [26]. LINFEI CHEN and DAOMU ZHAO [27] introduced a fractional wavelet packet based image encoding technique for color images. A new color image encoding technique using random phases in dual fractional Fourier-wavelet domain has been proposed by LINFEI CHEN and DAOMU ZHAO [28]. PRASAD *et al*. [29] have developed a color image encoding technique using discrete wavelet transform (DWT) in FrFT domain. The security of this work is good but it has a disadvantage because at encoder end it doubles the size of encrypted image which is not good from a transmission point of view. An image encryption technique is developed by LINFEI CHEN *et al*. [30] using SVD and Arnold transform in fractional Fourier domain. This work exhibits an increased level of security but transmits three encrypted images, what increases the transmission time and cost. For correct decryption, it is necessary to have all the three encrypted images along with the keys used for encryption. Recently, a novel image encoding technique using DWT and SVD in discrete orthonormal Stockwell transform (DOST) domain is proposed by KUMAR *et al*. [31, 32]. Although, the works reported in [29, 30] have achieved a desired level of security, the way of arrangement used in [29] doubles the size of encrypted image and the work reported in [30] has increased the transmission time and cost by transmitting three encrypted images of dimension equal to the dimension of the original image, which is not wanted from a point of view of transmission speed and storage. However, in our work, we have improved the security of images by overcoming the drawbacks of [29, 30].

In this paper, an improved image encryption technique using discrete cosine Stockwell transform (DCST) and singular value decomposition (SVD) is proposed. This work provides a more secure image encryption technique for secure transmission over the public networks. An original color image is decomposed into its primary color components, *i.e.*, red (R), green (G) and blue (B), then each of the R, G and B planes are encrypted independently using SVD in DCST domain. We have used bands of DCST, a parameter used to mask the values of singular values and the way of arrangement of SVD decomposed images as encryption keys. For correct decryption of encrypted images, correct knowledge of all the keys along with the way of arrangement is necessary.

The rest of the paper is organized as follows: Section 2 describes the terms related to the proposed work, the proposed encryption technique is discussed in Section 3, in Section 4, the experimental results on some standard test images are shown, comparison of proposed work with some related works is given in Section 5, Section 6 concludes the proposed work.

2. Related theories

2.1. Discrete cosine Stockwell transform

Stockwell transform (ST) is a time-frequency decomposition which gives absolutely-referenced phase information along with a progressive resolution. ST was developed to bridge the gap between Fourier and wavelet transforms. A discrete version of ST also exists but it suffers from a high redundancy problem. Further, a non-redundant version of ST also came into consideration that overcomes the problem of discrete ST and is termed as a discrete orthonormal Stockwell transform (DOST). DOST and its variants can be defined as combinations of Fourier transform (DFT). DOST is an energy preserving transformation because of its orthonormal and conjugate symmetry [33, 34] properties. The basis vector introduced by Stockwell [35] is constructed as a sum of Fourier basis vectors that are first shifted in time and then phase-corrected:

$$D_{v\beta\tau}[k] = \frac{\exp(i\Pi\tau)}{\sqrt{\beta}} \sum_{f = v - \frac{\beta}{2}}^{v + \frac{\beta}{2} - 1} \exp\left(-i\frac{2\Pi}{N}kf\right) \exp\left(i\frac{2\Pi}{\beta}\tau f\right) \tag{1}$$

where, v is the center of each frequency band, β is the width of the band, while τ represents the location in time [33]. As given in [36], DOST can be factored as the product of matrices D_i

$$\mathrm{DOST} = \left(\bigoplus_{i=1}^{k} D_i\right)\mathrm{DFT} \tag{2}$$

The direct sum of the matrices D_i results in a block-diagonal matrix, with each sub-block (D_i) as an altered inverse Fourier transform.

The above defined DOST can be modified by replacing the Fourier transform of Eq. (2) with discrete cosine transform (DCT). DCT plays a vital role in image processing, it is a real valued transform, which makes it suitable in many image processing techniques. A DCT based DOST can be derived by replacing DFT with DCT [36] as:

$$\mathrm{DCST} = \left(\bigoplus_{i=1}^{k} D_i\right)\mathrm{DCT} \tag{3}$$

The use of DCT in Eq. (3) results in all positive frequencies, and from all the positive frequencies, high frequencies are generally used for further processing.

2.2. Singular value decomposition

Singular value decomposition (SVD) is a very popular technique in linear algebra and is used in several applications of image processing. SVD [37–39] has an advantage of its applicability on both square and rectangular matrices. An image is basically a 2D matrix, where each and every cell represents a pixel value more specific to integer. SVD transformation decomposes an image A into three matrices U, S and V such as $A = USV^{\mathrm{T}}$ (where U and V are orthogonal matrices and S is a diagonal matrix containing singular values in a descending order). For an image of size $M \times N$, the orthogonal matrices U and V are of size $M \times M$ and $N \times N$, respectively, and the diagonal matrix S is of dimension $M \times N$, *i.e.*,

$$A_{M \times N} = U_{M \times M} S_{M \times N} (V_{N \times N})^{\mathrm{T}} \tag{4}$$

SVD is a method used to diagonalize the matrix [37]. It is also used to uncorrelate the correlated information, which uncovers the relationship among the pixels and gives uncorrelated data.

3. Proposed algorithm

The proposed encryption and decryption schemes are shown in Figs. 1 and 2, respectively. In the encryption phase, the original color image of size $M \times N$ is decomposed

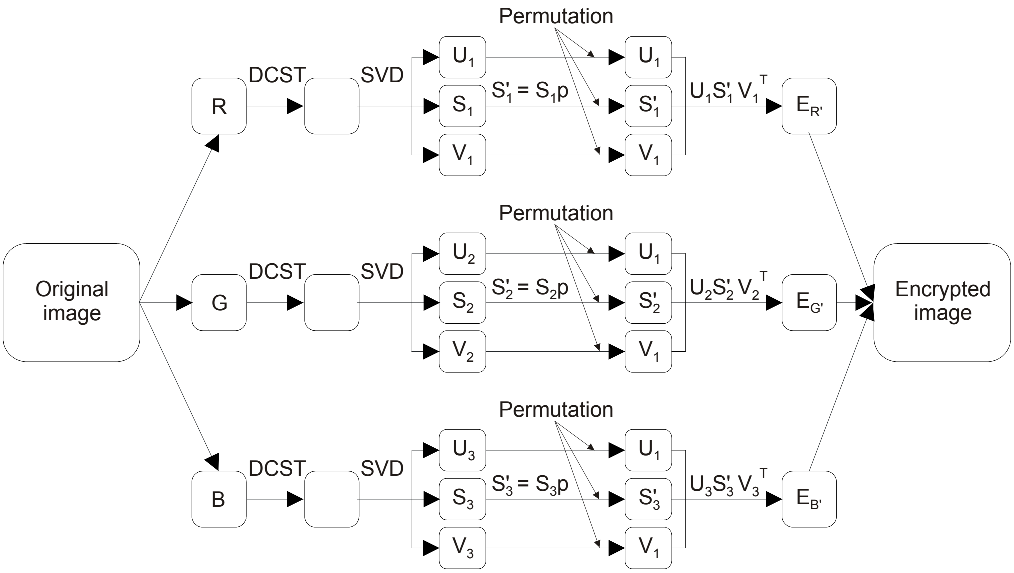

Fig. 1. Proposed encryption process.

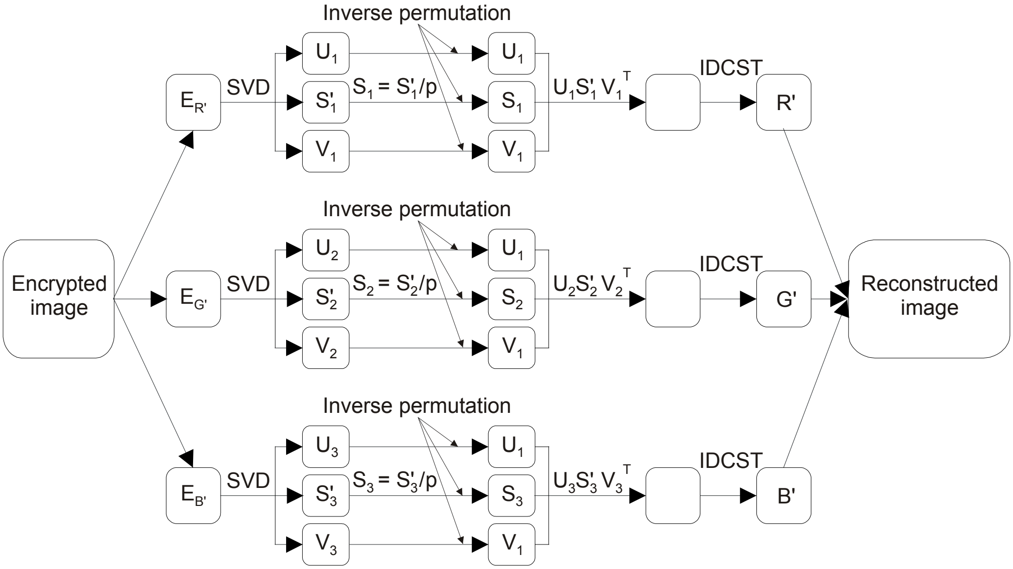

Fig. 2. Proposed decryption process.

into R, G and B planes. Each of the R, G and B plane is DCST transformed and further SVD is applied on all of the transformed planes, which gives U, S and V matrices corresponding to each of the plane. The singular values S of these planes are modified using a parameter p. Further, the modified singular values S' and other matrices of SVD are pseudo-randomly permuted. The pseudo-randomly encrypted images are reconstructed using new singular values (where $S' = Sp$). Several ways of permutation are reported in [40, 41], however, the way reported in [40] has been used in our work. The procedure for image decryption is just a reverse of encryption. All the decrypted R′, G′ and B′ planes are combined to get the reconstructed color image.

4. Experimental results and security analysis

The proposed scheme is applied on several test images each of size 512 × 512. The test images used in our work are shown in Fig. 3. Original *Barbara* and the encrypted images are shown in Figs. 4**a** and 4**b**, respectively. However, the correctly decrypted image is shown in Fig. 4**c**. It can be observed from Fig. 4**c** that the proposed work can decrypt the original image without any significant information losses.

The robustness of proposed work is analyzed on several test images and results are computed for each image. However, for demonstration purposes, a test image *Barbara* is used. An incorrectly decrypted *Barbara* image is shown in Fig. 5**a** when the number of bands used in DCST is incorrect. Figure 5**b** shows an incorrectly decrypted image when the way of permutation used is incorrect.

An incorrectly decrypted image using an incorrect number of DCST bands and incorrect arrangement of SVD images is shown in Fig. 6**a**. Figure 6**b** shows an incor-

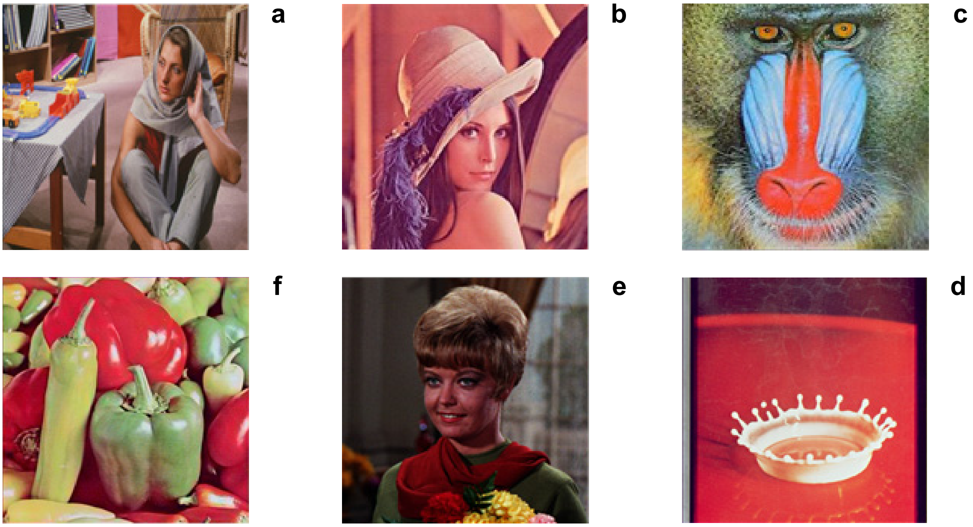

Fig. 3. *Barbara* (**a**), *Lena* (**b**), *Baboon* (**c**), *Peppers* (**d**), *Girl* (**e**), and *Splash* (**f**).

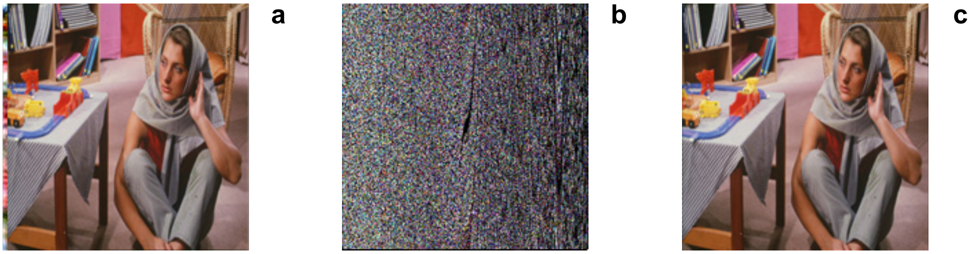

Fig. 4. Original (**a**), encrypted (**b**), and correctly decrypted (**c**) images.

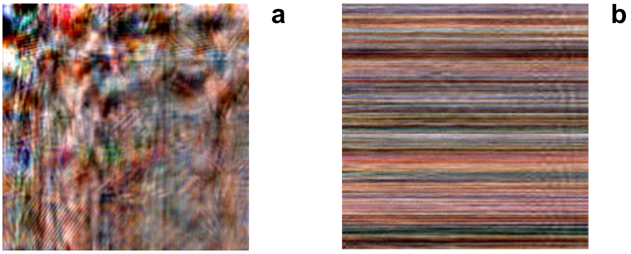

Fig. 5. Incorrect DCST bands (**a**), and incorrect way of permutation (**b**).

rectly decrypted image when the incorrect number of DCST bands and the way of permutation used are incorrect while Fig. 6**c** demonstrates an incorrectly decrypted image when SVD decomposed images are incorrectly arranged with an incorrect way of permutation. It can be analyzed from Figs. 6**a**–6**c** that the proposed work does not reveal the original image information if the incorrect parameters are used for decryption. In

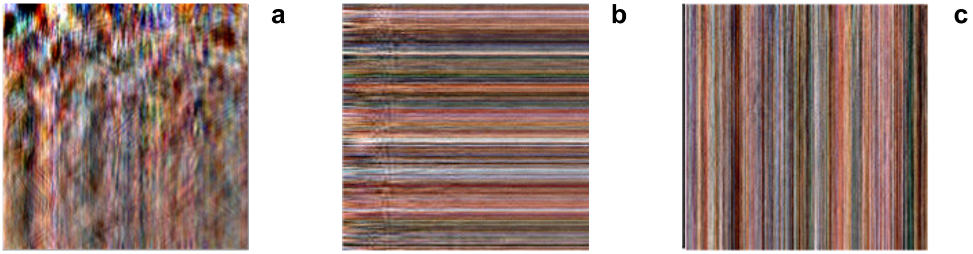

Fig. 6. Decrypted images: incorrect DCST bands with incorrect arrangement (SVU) (**a**), incorrect DCST bands with incorrect way of permutation (**b**), and incorrect SVD images with incorrect way of permutation (**c**).

our experiments, the incorrect values are chosen close to the correct ones and the parameter p is chosen to be 0.67. Figures 5 and 6 show the robustness against the change in one and two parameters, respectively. Hence, it is obvious that it will be even harder to recognize the incorrectly decrypted images when more than two parameters are wrong.

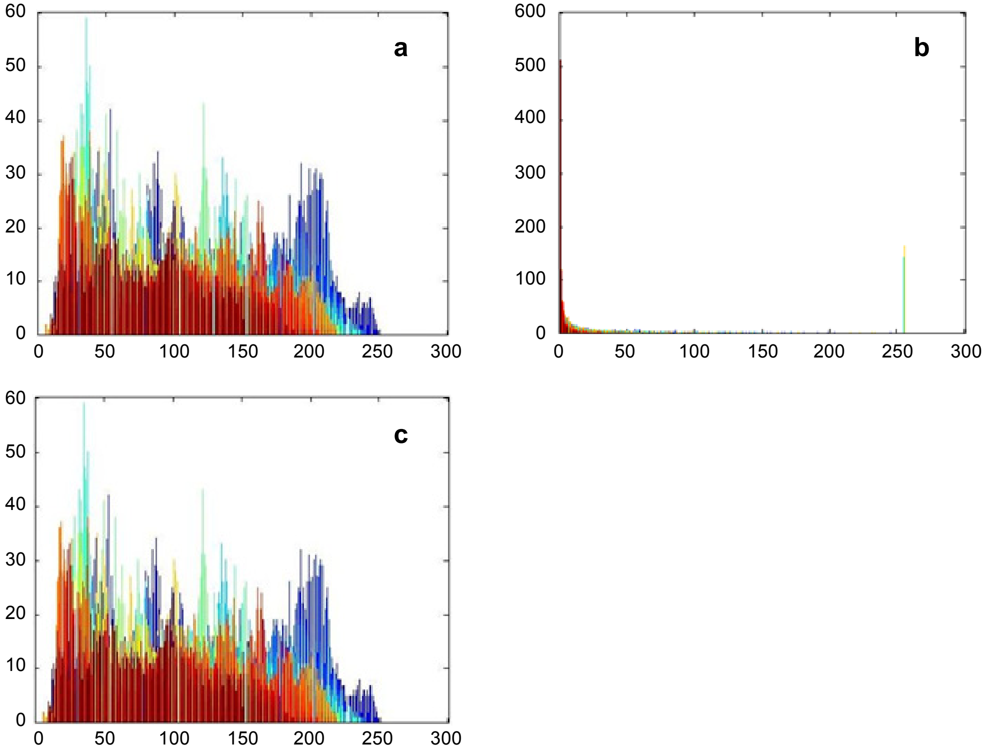

Fig. 7. Histogram of *Barbara* image (**a**), of encrypted *Barbara* image (shown in Fig. 4**b**) (**b**), and of correctly decrypted *Barbara* image (**c**).

4.1. Histogram analysis

The histogram of an image shows the distribution of intensity values in the three color planes, namely R, G and B. The histogram of original *Barbara* image is shown in Fig. 7**a** and the histogram of an encrypted image (shown in Fig. 4**b**) is shown in Fig. 7**b**. The histogram of correctly decrypted *Barbara* image using the proposed technique is shown in Fig. 7**c**. It can be seen from Fig. 7**b** that the histogram of the encrypted image is completely different from the histogram of Fig. 7**a**, which shows the effectiveness of the proposed work. However, Fig. 7**c** shows the histogram of the correctly decrypted image, which is almost identical to the original image (Fig. 7**a**).

4.2. Mean square error

The quality measure of the decrypted image can be calculated using mean square error (MSE) between the original I and correctly decrypted I' images. For an image of size $M \times N$ MSE can be defined as

$$\mathrm{MSE} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\Big[\left|I(m\Delta x, n\Delta y) - I'(m\Delta x, n\Delta y)\right|^{2}\Big] \tag{5}$$

where Δx and Δy represent the pixel size.

Table 1. Mean square errors of existing and proposed schemes for various test images.

Input image	RGB color planes	Scheme in [29]	Scheme in [30]	Scheme in [31]	Proposed scheme
Barbara	Red	$7{:}5757 \times 10^{-25}$	$1{:}2020 \times 10^{-29}$	2.5189×10^{-29}	5.8423×10^{-30}
	Green	$5{:}7824 \times 10^{-25}$	$1{:}2046 \times 10^{-29}$	4.3361×10^{-29}	8.8763×10^{-30}
	Blue	$4{:}9245 \times 10^{-25}$	$8{:}4432 \times 10^{-30}$	3.9424×10^{-29}	2.4052×10^{-30}
Lena	Red	1.6581×10^{-24}	4.5817×10^{-29}	2.7813×10^{-28}	1.1589×10^{-28}
	Green	3.6301×10^{-25}	7.5088×10^{-30}	8.7704×10^{-29}	4.8926×10^{-30}
	Blue	3.6723×10^{-25}	9.7892×10^{-30}	7.9489×10^{-29}	6.6693×10^{-30}
Baboon	Red	5.4772×10^{-25}	2.4168×10^{-29}	4.6729×10^{-29}	4.6020×10^{-31}
	Green	2.5581×10^{-25}	1.8396×10^{-30}	5.6848×10^{-29}	1.0287×10^{-30}
	Blue	6.5808×10^{-25}	7.3902×10^{-29}	5.9602×10^{-29}	9.0735×10^{-31}
Peppers	Red	1.2662×10^{-24}	2.2560×10^{-30}	2.6083×10^{-29}	4.9719×10^{-30}
	Green	2.1288×10^{-24}	9.9477×10^{-29}	4.9703×10^{-29}	9.5624×10^{-30}
	Blue	8.0634×10^{-25}	3.8857×10^{-30}	1.6758×10^{-29}	3.5328×10^{-30}
Girl	Red	2.3666×10^{-24}	3.8857×10^{-30}	3.3607×10^{-29}	3.7368×10^{-31}
	Green	1.4014×10^{-25}	5.3887×10^{-30}	1.6605×10^{-29}	6.1228×10^{-31}
	Blue	1.4152×10^{-25}	4.2230×10^{-30}	1.1964×10^{-29}	4.0551×10^{-31}
Splash	Red	1.6581×10^{-24}	5.3492×10^{-29}	6.2882×10^{-29}	2.4800×10^{-29}
	Green	1.6581×10^{-24}	4.6212×10^{-29}	4.2116×10^{-29}	9.0610×10^{-30}
	Blue	1.6581×10^{-24}	4.4682×10^{-29}	2.7299×10^{-29}	9.7355×10^{-30}

The proposed scheme is applied on several test images shown in Fig. 3 and MSE values for each of the correctly decrypted color planes are given in Table 1. It can be seen that the errors between the original and correctly decrypted images are very close to zero, which shows that the proposed work can decrypt the images without any recognizable information loss.

4.3. Structural similarity index metric

To evaluate the quality of reconstructed images, several measures are available such as PSNR and MSE. Another method was given by Zhou Wang *et al.* [42] to evaluate the quality of reconstructed images. The value of structural similarity index metric (SSIM) lies within the range of –1 to 1. If SSIM is 1, it shows that the reconstructed image is identical to the original one. Structural similarity of two images can be calculated as

$$\mathrm{SSIM} = \frac{(2\mu_I\mu_{I'} + C_1)(\sigma_{II'} + C_2)}{(\mu_I^2 + \mu_{I'}^2 + C_1)(\sigma_I^2\sigma_{I'}^2 + C_2)} \tag{6}$$

where μ_I and $\mu_{I'}$ are the averages corresponding to images I and I', respectively, while, σ_I^2 and $\sigma_{I'}^2$ represent the variances of images I and I', respectively; $\sigma_{II'}$ is the covariance between I and I' images, and C_1 and C_2 are the predefined constants. The SSIM values

Table 2. Structural similarity index metric (SSIM) between original and encrypted images of proposed scheme on various test images.

Input images	RGB color planes	SSIM
Barbara	Red	2.2848×10^{-4}
	Green	4.2981×10^{-4}
	Blue	8.0632×10^{-4}
Lena	Red	3.12805×10^{-5}
	Green	6.7437×10^{-4}
	Blue	4.2423×10^{-4}
Baboon	Red	-6.9999×10^{-5}
	Green	-1.4885×10^{-5}
	Blue	-2.1219×10^{-5}
Peppers	Red	1.7040×10^{-4}
	Green	0.0236
	Blue	0.0241
Girl	Red	0.0032
	Green	0.0573
	Blue	0.0348
Splash	Red	2.8819×10^{-4}
	Green	0.0435
	Blue	0.0011

between original and encrypted images are shown in Table 2. It can be observed from Table 2 that the proposed work gives enough security as the SSIM values between original and encrypted images are close to zero. We have calculated the SSIM values between the original and correctly decrypted images, and for all the test images, the calculated value is equal to 1, which means that the correctly decrypted images are almost identical to the original images.

5. Comparison of proposed work with some existing works

The effectiveness of proposed work is evaluated by comparing it with some related methods [29, 30] along with a recent published work on image security [31]. Our work has several advantages over existing works [29–31]; first, due to the use of DCST, the whole encryption process is performed in the real domain, while the works reported in [29–31] process the information complex domain, and it is very well know that the processing of information in the complex domain adds an extra overhead of dealing with real and imaginary parts separately. Second, as for the best of our knowledge, DCST along with SVD is used for the first time for image encryption, which may open a new direction. The use of SVD in DCST domain along with the masking of singular values and permutation gives more secure information than [29–31]. As described in Section 1, the arrangement used in [29] to obtain an encrypted image doubles the size of encrypted image that increases the transmission time and cost of storage. In [30] three encrypted images are transmitted of the size equal to the original image, which also increases an extra overhead of transmission of each of the three encrypted images. Thus, the work given in [29, 30] achieves good security but work reported in [29] doubles the size of the encrypted image, while [30] transmits three encrypted images, which is not good from the transmission point of view. Apart from this, we have also compared our work with a recently published work [31] which is based on DOST. This work has overcome the disadvantages of [29, 30] but it also processes the information in the complex domain as reported in [29, 30]. Hence, the proposed work processes the information in the real domain rather than complex, which has reduced the overhead of processing of real and imaginary parts separately. The proposed scheme also overcomes the disadvantages of these existing works [29, 30] by transmitting a single encrypted image of dimension equal to the original image with increased security. The robustness of the proposed work against incorrect parameters shows the efficiency of the proposed encryption scheme. It can be noticed from Table 1 that the proposed scheme can decrypt the encrypted images more efficiently as the MSE values between original and correctly decrypted images of the proposed work are smaller than the MSE values of works reported in [29–31]. However, the structural similarity between the original and encrypted images on various test images is shown in Table 2. It can be observed from Table 2 that the proposed scheme provides more secure information as the SSIM values between original and encrypted images are close to 0, which indicates that there is almost no similarity between original and encrypted images.

6. Conclusions

In this paper, an improved color image encryption technique has been proposed using SVD in DCST domain. The salient attributes of SVD in DCST domain along with the way of permutation used provide more secure information. For correct decryption of encrypted images, it is indeed necessary to have correct knowledge of all the keys along with the exact values. The robustness analysis of our work has shown that if a single parameter is incorrect, and the other parameters are correct it is nearly impossible to guess the original image information. Hence it is necessary to have correct knowledge of all the keys in correct order for correct decryption. The effectiveness of the proposed work is analyzed by comparing it with some related works and it is found that the proposed work can provide more secure information with less information loss as the MSE values of the proposed work are smaller in comparison to existing works. However, the SSIM between the original and encrypted images show that the proposed work can transmit the encrypted images without revealing the original image information.

References

[1] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters 20(7), 1995, pp. 767–769.

[2] JAVIDI B., NOMURA T., *Securing information by use of digital holography*, Optics Letters 25(1), 2000, pp. 28–30.

[3] SINGH N., SINHA A., *Optical image encryption using Hartley transform and logistic map*, Optics Communications 282(6), 2009, pp. 1104–1109.

[4] LINFEI CHEN, DAOMU ZHAO, *Optical image encryption with Hartley transforms*, Optics Letters 31(23), 2006, pp. 3438–3440.

[5] ZHENGJUN LIU, YU ZHANG, WEI LIU, FANYI MENG, QUN WU, SHUTIAN LIU, *Optical color image hiding scheme based on chaotic mapping and Hartley transform*, Optics and Lasers in Engineering 51(8), 2013, pp. 967–972.

[6] QING GUO, ZHENGJUN LIU, SHUTIAN LIU, *Color image encryption by using Arnold and discrete fractional random transform in IHS space*, Optics and Lasers in Engineering 48(12), 2010, pp. 1174–1181.

[7] ZHENGJUN LIU, LIE XU, TING LIU, HANG CHEN, PENGFEI LI, CHUANG LIN, SHUTIAN LIU, *Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains*, Optics Communications 284(1), 2011, pp. 123–128.

[8] ZHENGJUN LIU, MIN GONG, YONGKANG DOU, FENG LIU, SHEN LIN, AHMAD M.A., JINGMIN DAI, SHUTIAN LIU, *Double image encryption by using Arnold transform and discrete fractional angular transform*, Optics and Lasers in Engineering 50(2), 2012, pp. 248–255.

[9] SINGH N., SINHA A., *Gyrator transform-based optical image encryption using chaos*, Optics and Lasers in Engineering 47(5), 2009, pp. 539–546.

[10] ABUTURAB M.R., *Color image security system using double random-structured phase encoding in gyrator transform domain*, Applied Optics 51(15), 2012, pp. 3006–3016.

[11] ABUTURAB M.R., *Securing color information using Arnold transform in gyrator transform domain*, Optics and Lasers in Engineering 50(5), 2012, pp. 772–779.

[12] ABUTURAB M.R., *Securing color image using discrete cosine transform in gyrator transform domain structured-phase encoding*, Optics and Lasers in Engineering 50(10), 2012, pp. 1383–1390.

[13] ABUTURAB M.R., *Color image security system based on discrete Hartley transform in gyrator transform domain*, Optics and Lasers in Engineering 51(3), 2013, pp. 317–324.

[14] Abuturab M.R., *Noise-free recovery of color information using a joint-extended gyrator transform correlator*, Optics and Lasers in Engineering 51(3), 2013, pp. 230–239.

[15] Abuturab M.R., *Color information verification system based on singular value decomposition in gyrator transform domains*, Optics and Lasers in Engineering 57, 2014, pp. 13–19.

[16] Nanrun Zhou, Yixian Wang, Lihua Gong, *Novel optical image encryption scheme based on fractional Mellin transform*, Optics Communications 284(13), 2011, pp. 3234–3242.

[17] Nanrun Zhou, Haolin Li, Di Wang, Shumin Pan, Zhihong Zhou, *Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform*, Optics Communications 343, 2015, pp. 10–21.

[18] Nanrun Zhou, Shumin Pan, Shan Cheng, Zhihong Zhou, *Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing*, Optics and Laser Technology 82, 2016, pp. 121–133.

[19] Nanrun Zhou, Aidi Zhang, Fen Zheng, Lihua Gong, *Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing*, Optics and Laser Technology 62, 2014, pp. 152–160.

[20] Nanrun Zhou, Aidi Zhang, Jianhua Wu, Dongju Pei, Yixian Yang, *Novel hybrid image compression–encryption algorithm based on compressive sensing*, Optik – International Journal for Light and Electron Optics 125(18), 2014, pp. 5075–5080.

[21] Lihua Gong, Xingbin Liu, Fen Zheng, Nanrun Zhou, *Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique*, Journal of Modern Optics 60(13), 2013, pp. 1074–1082.

[22] Yu-Guang Yang, Juan Xia, Xin Jia, Hua Zhang, *Novel image encryption/decryption based on quantum Fourier transform and double phase encoding*, Quantum Information Processing 12(11), 2013, pp. 3477–3493.

[23] Nan Run Zhou, Tian Xiang Hua, Li Hua Gong, Dong Ju Pei, Qing Hong Liao, *Quantum image encryption based on generalized Arnold transform and double random-phase encoding*, Quantum Information Processing 14(4), 2015, pp. 1193–1213.

[24] Zhengjun Liu, Shutian Liu, *Random fractional Fourier transform*, Optics Letters 32(15), 2007, pp. 2088–2090.

[25] Shutian Liu, Quanlin Mi, Banghe Zhu, *Optical image encryption with multistage and multichannel fractional Fourier-domain filtering*, Optics Letters 26(16), 2001, pp. 1242–1244.

[26] Yan Zhang, Cheng-Han Zheng, Naohiro Tanno, *Optical encryption based on iterative fractional Fourier transform*, Optics Communications 202(4–6), 2002, pp. 277–285.

[27] Linfei Chen, Daomu Zhao, *Image encryption with fractional wavelet packet method*, Optik – International Journal for Light and Electron Optics 119(6), 2008, pp. 286–291.

[28] Linfei Chen, Daomu Zhao, *Color image encoding in dual fractional Fourier-wavelet domain with random phases*, Optics Communications 282(17), 2009, pp. 3433–3438.

[29] Prasad A., Kumar M., Choudhury D.R., *Color image encoding using fractional Fourier transformation associated with wavelet transformation*, Optics Communications 285(6), 2012, pp. 1005–1009.

[30] Linfei Chen, Daomu Zhao, Fan Ge, *Image encryption based on singular value decomposition and Arnold transform in fractional domain*, Optics Communications 291, 2013, pp. 98–103.

[31] Kumar M., Agrawal S., *Color image encoding in DOST domain using DWT and SVD*, Optics and Laser Technology 75, 2015, pp. 138–145.

[32] Kumar M., Vaish A., *Encryption of color images using MSVD in DCST domain*, Optics and Lasers in Engineering 88, 2017, pp. 51–59.

[33] Wang Y., *Efficient Stockwell Transform with Applications to Image Processing*, Ph.D. Thesis, University of Waterloo, Ontario, Canada, 2011.

[34] Stockwell R.G., *A basis for efficient representation of the S-transform*, Digital Signal Processing 17(1), 2007, pp. 371–393.

[35] Ladan J., *An Analysis of Stockwell Transforms, with Applications to Image Processing*, Ph.D. Thesis, University of Waterloo, Ontario, Canada, 2014.

[36] LADAN J., VRSCAY E.R., *The discrete orthonormal Stockwell transform and variations, with applications to image compression*, [In] Kamel M., Campilho A. [Eds.], *Image Analysis and Recognition. ICIAR 2013. Lecture Notes in Computer Science*, Vol. 7950, Springer, Berlin, Heidelberg, pp. 235–244.

[37] KAMM J.L., *SVD-based methods for signal and image restoration*, Ph.D. Thesis, 1998.

[38] RANADE A., MAHABALARAO S.S., KALE S., *A variation on SVD based image compression*, Image and Vision Computing 25(6), 2007, pp. 771–777.

[39] KUMAR M., VAISH A., *An efficient encryption-then-compression technique for encrypted images using SVD*, Digital Signal Processing 60, 2017, pp. 81–89.

[40] BOURBARKIS N., ALEXOPOULOS C., *Picture data encryption using scan patterns*, Pattern Recognition 25(6), 1992, pp. 567–581.

[41] YEN J.-C., GUO J.-I., *Efficient hierarchical chaotic image encryption algorithm and its VLSI realization*, IEE Proceedings – Vision, Image and Signal Processing 147(2), 2000, pp. 167–175.

[42] ZHOU WANG, BOVIK A.C., SHEIKH H.R., SIMONCELLI E.P., *Image quality assessment: from error visibility to structural similarity*, IEEE Transactions on Image Processing 13(4), 2004, pp. 600–612.

Received April 8, 2017
in revised form May 30, 2017