Taylor & Francis
Taylor & Francis Group

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: 0005-1144 (Print) 1848-3380 (Online) Journal homepage: https://www.tandfonline.com/loi/taut20

Dynamic virtual cluster cloud security using hybrid steganographic image authentication algorithm

K. Venkatraman & K. Geetha

To cite this article: K. Venkatraman & K. Geetha (2019) Dynamic virtual cluster cloud security using hybrid steganographic image authentication algorithm, Automatika, 60:3, 314-321, DOI: 10.1080/00051144.2019.1624409

To link to this article: https://doi.org/10.1080/00051144.2019.1624409

Published online: 12 Jun 2019.

AUTOMATIKA
2019, VOL. 60, NO. 3, 314–321
https://doi.org/10.1080/00051144.2019.1624409

SPECIAL ISSUE: COMPUTATIONAL INTELLIGENCE AND CAPSULE NETWORKS

Dynamic virtual cluster cloud security using hybrid steganographic image authentication algorithm

K. Venkatraman[a] and K. Geetha[b]

[a]Anna University, Chennai, India; [b]Department of Computer Science & Engineering, Excel Engineering College, Anna University, Komarapalayam, India

ABSTRACT

Storing data in a third party cloud system causes serious problems on data confidentiality. Generally, encryption techniques provide data confidentiality but with limited functionality, which occurs due to unsupported actions of encryption operation in cloud storage space. Hence, developing a decentralized secure storage system with multiple support functions like encryption, encoding, and forwarding tends to get complicated, when the storage system spreads. This paper aims mainly on hiding image information using specialized steganographic image authentication (SSIA) algorithm in clustered cloud systems. The SSIA algorithm is applied to virtual elastic clusters in a public cloud platform. Here, the SSIA algorithm embeds the image information using blowfish algorithm and genetic operators. Initially, the blowfish symmetric block encryption is applied over the image and then the genetic operator is applied to re-encrypt the image information. The proposed algorithm provides an improved security than conventional blowfish algorithm in a clustered cloud system.

ARTICLE HISTORY
Received 18 January 2019
Accepted 29 April 2019

KEYWORDS
Genetic algorithm; encryption; blowfish algorithm; cloud security; steganography

1. Introduction

In recent years, cloud computing gained a better recognition in organization and individuals using storage, computation, and software services [1]. The cloud computing faces multiple challenges, some include auditability, lock-in, transfer problems, confidentiality, unpredictability, performance, storage scalability, bugs, and software licensing [2]. The main risk in cloud computing is its privacy, interoperability, and compatibility [3]. The owner is unaware to control the data privacy and the issues of security and privacy related to data integrity, availability of service, and intrusion in data [4].

The main drawback associated with cloud computing is its issues related to security and privacy of data. Since, cloud computing is an important application in health, banking, and security services [5–7], the data is considered sensitive. Hence, better confidentiality has to be maintained at the user and server side during processing, rest, and transfer. This has imposed the present study to consider data security as an important and critical issue that has to be addressed thoroughly. The present research deals with analysing the security using steganographic encryption procedure in cluster-based cloud data model.

In the proposed system, the cloud computing security is improved using secured cryptosystem. The modules of steganography security are different for cloud system and general systems, especially in distributed computing. The main feature of the steganography model is that it is possible to make the model work under various sites of the distributed system [8]. For cloud computing, the attacks on steganography operation relate to side channel attacks. To make the steganography algorithm to operate on cloud, the cloud system should provide better elastic services and better support of the steganography algorithm on a cloud environment.

The cryptosystem used is steganography based system, which is designed to work on the distributed data and further, it accumulates and reduces the data loss with increased efficiency without any security loss. The efficiency of the proposed system is computed on both high-performance computation and usage of valuable resource while designing key and random sequence. Careful measures are considered in the proposed study and the proposed method is modelled with machine learning steganography approaches.

In this paper, a domain-specific model is proposed to encrypt the images. The major contributions of this work is discussed as follows:

(i) The blowfish algorithm is used for steganographic encryption and genetic algorithm is used to encrypt the image further using crossover and mutation operators during image distribution.

CONTACT K. Venkatraman kvrforu@gmail.com Anna University, Chennai 600025, India

(ii) The novel contribution is the usage of steganographic hybrid encryption which is adopted in cluster-based cloud environment to improve the security of images.
(iii) Here, the security is ensured by GA and the BA is utilized to reduce the computations involved in encrypting and decrypting the message.

The outline of the paper is organized as follows: Section 2 provides the related works. Section 3 discusses the proposed hybrid algorithm and the stages of encryption. Section 4 evaluates the performance of the proposed algorithm. Section 6 concludes the work.

2. Related work

To ensure confidentiality or privacy and to make reliability on storage data, various mechanisms are proposed by the researchers. In [9], a novel authentication scheme is used to combine text and graphical passwords for better access control. The first round of graphical authentication is a recognition technique and the second round is a recall technique. A next step is a behavioural study of the user and this approach offers highly secured systems in real time. In [10], an implicit password authentication system is used, where authentication is presented to the user. If the user "clicks" the grid-of-interest compared with the server, consumer and user are authenticated for using the services. No password information is exchanged between the client and the server. Since the authentication information is conveyed implicitly, this system tolerates shoulder surfing and screen dump attack. The main advantage lies in creating a better authentication space with a large collection of images to avoid short repeating cycles. Image encryption schemes meet the demand for real-time secure image transmission over the Internet [11]. The security of the digital image is important due to the rapid evolution of the Internet.

Homomorphic encryption [12] is a cryptographic tool used widely for improved security in cloud computing. This makes the cloud to operate on specific computation like encryption, ciphertext generation, and decryption. It provides privacy and security to the cloud outsourced data and storage. In [13], homomorphic encryption is used to encode the image with direct operation. It suffers mainly from resource constraints since the encryption is performed mostly on the client side with high computational overhead. Proxy re-encryption [14] secures the data sharing in cloud and delegates the capability of proxy re-encryption. The re-encrypt is taken place by the re-encryption key. Time-proxy re-encryption scheme [15] does not allow the client to encrypt the data and this avoids computational limitations during the use of resource-based constraint. Secure multiparty computation [16] enables different parties for computing on the same function and maintains the inputs, private. The other schemes related to secure multiparty computation in image processing is seen in [17,18]. However, it does not fit with thin clients, since parties involve in computational overhead due to symmetry property. Convectional cryptographic encryption models are proposed in [19] to encrypt the plain image before sending it over the cloud. It includes lossy image compression [20] with compressive sensing, template matching [21], image masking, and splitting. Steganography technique in [22] stores the images in the cloud. It could be concluded that there are several techniques available to encrypt the data storage in a cloud environment using proxy re- and homomorphic encryption.

However, the proposed technique does not fit with the above technique, since the operation involves the encryption of images inside the cluster cloud network and further the resource is user limited. The secure multiparty computing can be used in such a hybrid cloud; however, the cost of operation at the client side is still expensive. Here, many steganography techniques [23,24] for image encryption is studied, but adoption in the cloud environment [20] is still less. The studies failed to report the hiding of images during its distribution over the cloud. Computation on such steganography image is not available in conventional literature.

3. Proposed algorithm

The proposed method is intended to provide proper authentication of images in the hybrid cluster cloud system. The high-level security is attained by using a dual encrypting algorithm or SSIA algorithm. This algorithm uses blowfish technique to encrypt the

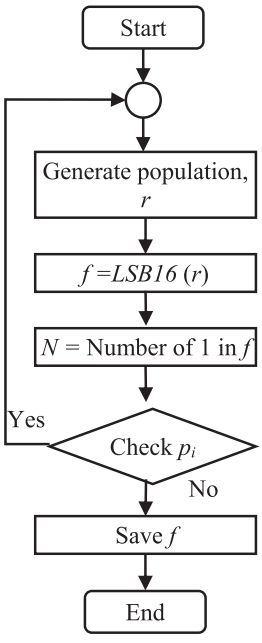


Figure 1. Random number generation.

image information and then the genetic operators like crossover and mutation is used to encrypt the encrypted parent individuals. The subkeys of the blowfish are stored in the cloud storage which avoids unauthorized access. This method avoids the selection of random individuals to encrypt the images since it is difficult to decrypt the images by the third party. However, a random number is utilized for the following purposes: (1) to encrypt the plain text with xor operation and (2) to reduce the total rounds in the blowfish algorithm.

Initially, a new random number is generated by the selection of a new random number by genetic algorithm from the whole set of population. The random number generated is of 64 bits and it checks for minimum five ones in the least significant bits of the random number, usually 16 bits. The generation of the random number is shown in Figure 1. Depending on the position of the ones in random number i.e. least significant 16 bits, the function F is executed. If the least significant 16 bits have zeros then the rounds will not be executed. Now, check the condition P_i lesser than 16, since the output of N is 16. When the condition is true, the loop goes from the initial condition of generating population, on the contrary, the random number obtained from f is stored.

The operation of two-tier encryption by the blowfish and genetic algorithm is shown in Figure 2. This leads to severe variation in function F during the process of executing the encryption and decryption function. This method resists the attacks at any stages or rounds since it executes five rounds using blowfish and the final rounds are done genetically. The proposed method thus has an integrated SSIA algorithm to provide high-level security to the images in the private cloud.

3.1. Blowfish algorithm

Blowfish algorithm is a symmetric operation, which is used for both encryption and data protection in high-end system. The algorithm operates on a key length of 32 bits, variable in its manner and it extends till 448 bits. This is considered supreme for protecting the data in the cloud environment.

This is a 16-round Feistel cipher with 4 key-dependent S-boxes. The scheduling procedure of key is done by initializing both the S-box and P-box and the

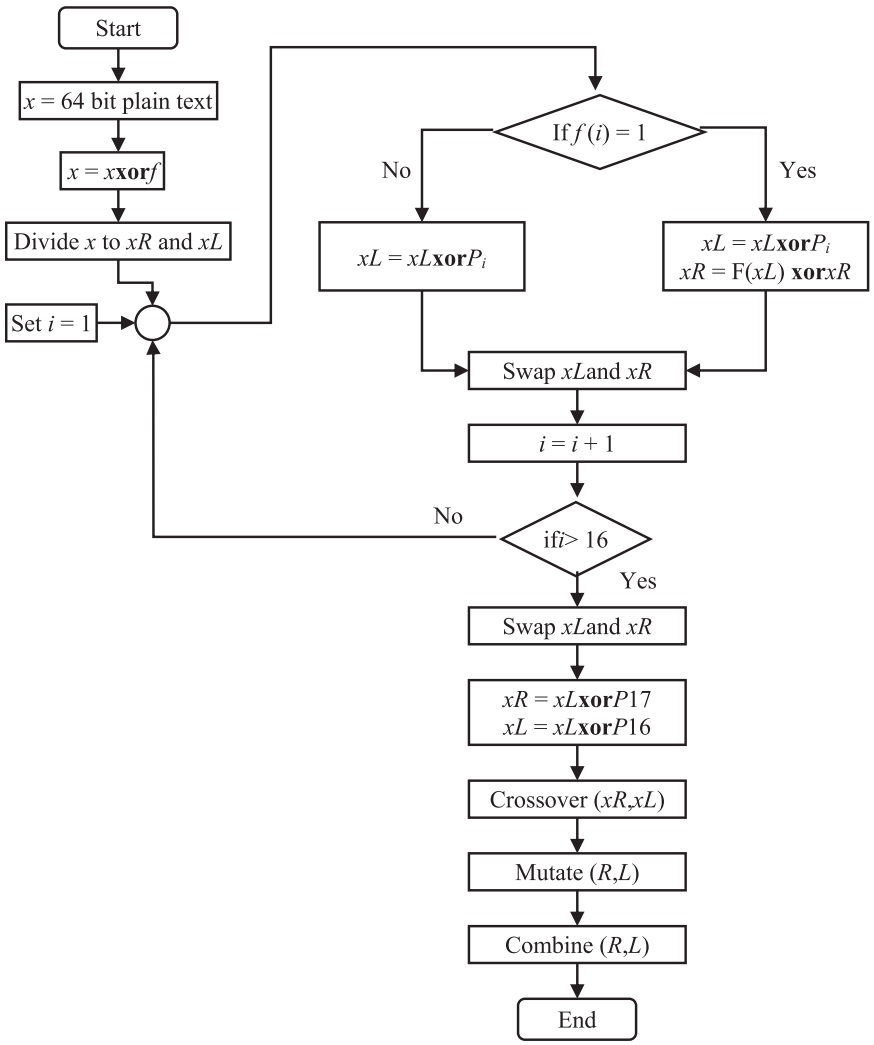


Figure 2. Proposed algorithm using blowfish-genetic operator.

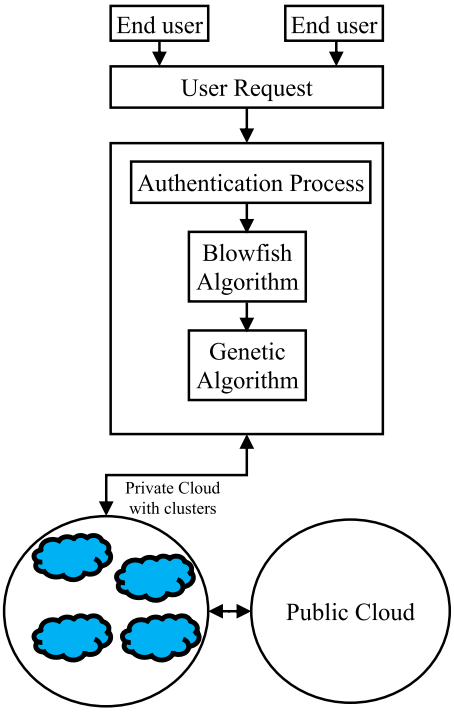


Figure 3. Proposed system architecture.

values are obtained from hexadecimal digits of p_i with an improper pattern, respectively. The P-box entries are XORed with the secret key to improve the encryption process. When the value of i is lesser than 16, the process gets back to the initialization step, where $f(i)$ is the considered one to acquire xL and xR, otherwise only xL is computed. On the other hand, when the value of i is greater than 16, then the process shifts to final operations like swapping, second level encryption, crossover, mutate, and combination of child individuals.

From Figure 3, the matrix value of each pixel value is obtained. The matrix values are used to obtain the RGB plane and it is dissected vertically into two halves, xR and xL. Each half is of 32 bits and the keys of two halves are encrypted individually using a user-defined key. The encrypted planes are then retrieved by concatenating vertically the two halves, xR and xL. The encrypted RGB planes are then merged together for constructing the final image, which is passed to the next stage of genetic operation.

3.1.1. Operation of blowfish algorithm

The entire blowfish operation takes place under 16 rounds. Initially, a random number is generated and then the given input image of 64-bit element is generated. Then, the random number is XORed with the input data. The x is divided into two equal halves, each of 32 bit size, namely, xL, xR.

3.2. Genetic algorithm

Genetic algorithm searches the individuals based on the probability and it solves the problem associated with optimization. This paper assigns the individuals to encrypt the given images using crossover and mutation operators. Also, the selection of individuals for random numbers is based on natural selection procedure. The main steps of the proposed genetic model have initial random number generation and assessment of individuals, obtained from the blowfish algorithm. It involves computing parent after selection from blowfish and production of offspring. Then, the child is allowed to mutate and next generation is chosen.

The generated chromosomes or random number from the entire set of population has a gene of different variants. Then, the suitable fitness function is assigned to assess the chromosome since it is a natural selection process, the higher fitness chromosome individuals are chosen for the next generation and then it is XORed with the input values. Finally, it produces children and proved to be fittest in terms of the initial fitness function.

The main aim is to find the optimal value of such element. Here, each chromosome has genes that are referred to as variables or element. Due to the natural selection process, the chromosome of parents competes with each other, depending on the fitness function. The higher compatibility objective function reproduces with higher probabilities based on following equation 1,

$$P(i) = \frac{\text{Fitness}(i)}{\sum_i \text{Fitness}(i)} \tag{1}$$

The ith probability of chromosome is denoted as P, with fitness value of the chromosome is denoted by *Fitness*. Finally, the child chromosomes from the two parent genes are shown in equation 2, 3,

$$xL = \alpha P_1 + (1 - \beta)P_2 \tag{2}$$

$$xR = (1 - \alpha)P_1 + \beta P_2 \tag{3}$$

where xL and xR are the child chromosomes and P_1 and P_2 are the parent chromosomes. Here, α and β are the constant values, where the values lie between 0 and 1.

During mutation, the parent chromosome from the blowfish stage of random position interchanges, in terms of its bits. The main aim is to increase the fitness of the chromosome, so that when the chromosome stay fit when the image pixels are shuffles and the pixel correlation stays least.

3.3. Blowfish image decryption

The output of the combined bits are given as an input to the blowfish decryption, which operated in the reverse way of the encryption mode; however, the order of the rounds is operated in a reverse way.

Appendix

Generate random number, R
Send R to an input image to generate 64-bit element, x
Divide x into $xL$and xR,
For $i = 1$–16 //Check Figure 3
If $f(i) = 1$ //Check Figure 3
$xL = xL$**xor**P_i //P-array is XORed with keybits, $xL//P_i$ is the P-array with i^{th} iterations
$xR = F(xL)$ **xor**xR // the function of xL is XORed with xR
//The function F is calcualted as follows,
Divide xL into four quarters a,b,c,d.
Calculate $F(xL) = ((S1,a + S2,b \bmod 232)$ xor $S3,c) + S4, d \bmod 232$
Else
$xL = xL$**xor**P_i //P-array is XORed with keybits, xL //P_i is the P-array with i^{th} iterations
End
Swap the 23 bits xL and xR
Swap the 23 bits xL and xR (Undo the last swap) //The new output 1 and 2 is obtained after swapping
Then,
$xR = xR$**xor**$P17$ //Encrypt again the swapped outputs with modified subkey$P17$
$xL = xL$**xor**$P18$ //Encrypt again the swapped outputs with modified subkey$P18$
//New output is obtained
Crossover the child (xR, xL) //Genetic crossover is carried out on new outputs
Mutate the Parent (R, L) //The parent individuals are mutated to obtain child individuals
Recombine (L, R) //Recombination of child individuals takes place
End

4. Proposed cloud stegnographic image authentication model

The proposed security model on cluster private cloud shares the image data in a dynamic way over the untrusted cloud. The proposed model preserves the data and identity. The unauthorized access of the data is prevented using hybrid stegnographic model with improved security in the private cloud. This is attained using the edge detection technique, which reduces further the key size and computational complexity. The data is accessed by the end user and it is not authorized to be used by the other data owners. The proposed data cloud model is shown in Figure 3.

The proposed SSIA algorithm is intended to share the user data in clusters and provides privacy and security when it is been distributed over the cloud. SSIA algorithm had embedded image like image steganography; however, an edge detection method is used for edge detection, where the user data is hidden. Prior to hiding the cover image data, confidentiality method is used to encrypt the data using the above blowfish-genetic operator.

The ciphertext while encrypting an image depends on the key with high quality, perfect selection, and design, since the adjacent pixel arrangement in the transposition cipher is disturbed and rearrangement pattern selects the encryption quality. The key is used to derive the rearrangement pattern and the quality of encryption is improved with the proper key. The rearrangement of n-pixel blocks is done using a key with n numbers of $n!$ patterns. The genetic algorithm is used to improve the search pattern for obtaining the optimal value.

In the proposed method, the best chromosome is affected heavily by the image pixel correlation. Here, the chromosome of size 16 is considered and the elements are integers, which indicates the updated position by the image pixel with a block size of 16. Each integer of the element in the chromosome is said to exist between the values of 1 and 16. The integer k on the chromosome (left) is considered as the new position, which is been assigned to pixel (k) inside the string of chromosome. The fitness function is used to evaluate how fit the chromosomes is, which is given in equation 1.

The proposed method uses the initial pre-processing operation to improve image encryption in an effective way. The image blocks are applied with the scrambling technique for pre-encryption process. Then, the image is broken down into small square blocks with 90 deg phase shift along the counter-clockwise direction, which has been flipped upside down. Finally, the transformed image is obtained from such shuffled blocks using the chaotic generator.

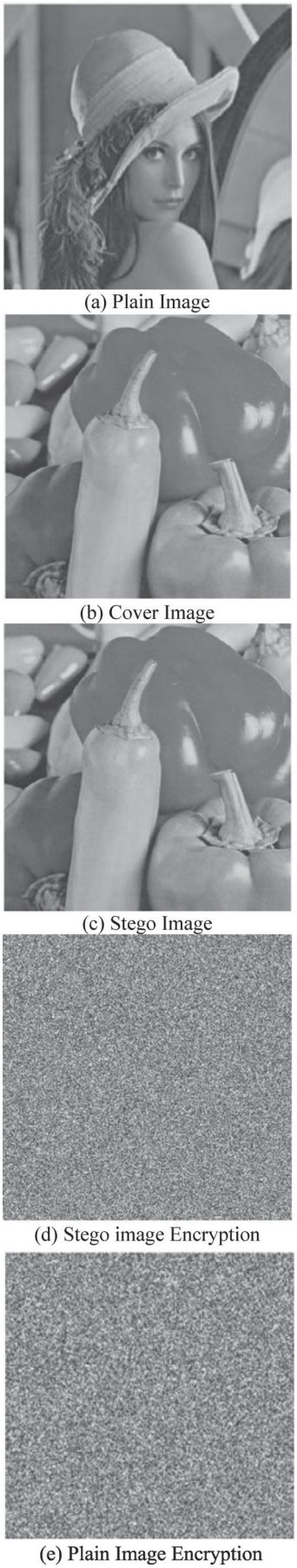
5. Experimental results

The proposed encryption algorithm is applied on Lena image. To check the effectiveness of the proposed SSIA algorithm, the correlation between the pixel blocks is tested. Initially, the pre-processing is carried out to obtain the transformed image. Then, RGB output images using blowfish and genetic algorithm is encrypted and analysed the performance of security over private cloud clusters. The results of encryption are shown in Figure 4.

5.1. NPCR and UACI

The proposed method uses double-layer encryption model, which is evaluated using pixels changing rate (NPCR), unified average changing intensity (UACI), and correlation co-efficient (CC).

The parameters, NPCR and UACI, have used security analysis during the process of image encryption.



(a) Plain Image

(b) Cover Image

(c) Stego Image

(d) Stego image Encryption

(e) Plain Image Encryption

Figure 4. Encryption results.

NPCR checks the pixel's absolute number and UACI checks the average difference between the cipher images (two pairs). The encryption technique is proved efficient if the value of NPCR is high and the value of UACI is low.

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{T} \times 100\% \tag{4}$$

$$\text{UACI} = \frac{\sum_{i,j} C_1(i,j) - C_2(i,j)}{FT} \times 100\% \tag{5}$$

where C_1 and C_2 are the cipher images and D is the bipolar array, T is the total pixels in cipher image, and F is the largest pixel value in cipher image. PVAL is the qualitative NPCR/UACI and SCR is the quantitative NPCR/UACI.

The values of the NPCR and UACI for the encryption using blowfish algorithm is shown in Tables 1 and 2. Similarly, the NPCR and UACI for the encryption using the proposed algorithm is shown in Tables 3 and 4.

5.2. Correlation coefficient

The correlation between the Lena images for encryption and decrypted image is shown in Table 2. From the results, it is seen that the proposed algorithm attains a better correlation than the blowfish alone. This is due to the fact that the proposed algorithm selects optimally the image pixels using a genetic algorithm.

5.3. Execution time

The execution time of the proposed system is compared with other conventional methods, shown in Table 3.

From the table, it is concluded that the proposed method attains a lesser execution time for encryption and decryption than the existing techniques like adaptive LSB substitution [25], adaptive neural networks [26], and iterative magic matrix encryption algorithm [25]. The simpler computation process attains a lesser execution time in the proposed system than the other methods, where all the three methods possess higher computational process.

5.4. PSNR

PSNR is used to test the difference between the original and processed image and it is considered as a main criterion to identify the image quality. The stego quality of the images under steganographic method with various embedding rate is estimated using the messages, which is embedded into 1000 cover and 1000 stego images. The PSNR results between cover and stego images is

Table 1. NPCR color components of the proposed system with blowfish algorithm.

		NPCR color components			
Techniques	Evaluation parameter	R	G	B	Entire image
NCPR value of blowfish algorithm	SCR	0.99632	0.9956	0.998291	0.99674
	PVAL	0.59889	0.308192	0.987914	0.876356
NCPR value of proposed algorithm	SCR	0.34917	0.340178	0.33929	0.34288
	PVAL	8.45E-05	0.133793	0.208028	1.12E-04
UACI value of blowfish algorithm	SCR	0.997314	0.993408	0.996093	0.995605
	PVAL	0.500000	0.691807	0.401104	0.557494
UACI value of proposed algorithm	SCR	0.341224	0.303878	0.282368	0.309157
	PVAL	0.001327	0.001327	0.001327	1.12E-04

Table 2. Correlation coefficient.

	Image	R	G	B	Entire image
Blowfish	Encrypted	0.029	−0.039	0.015	−0.006
	Decrypted	1	1	1	1
Proposed algorithm	Encrypted	−0.0179	−0.0129	−0.0014	−0.0009
	Decrypted	1	1	1	1

shown in Figure 4.

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{(2^d-1)^2}{mse}\right]$$

where d is the number of bits for representing the samples. Further, the mse is the mean of m_k values over entire image blocks:

$$mse = \frac{1}{N}\sum_{k=1}^{N} m_k$$

and m_k is the mean square error between the blocks, which is given by

$$m_k = \frac{1}{n}\sum_{i=1}^{n}(x_i^k - y_i^k)^2$$

where $k = 1, 2, \ldots, N$.

From the results of Table 4, it is found that the proposed system attains better results than the conventional methods. This is due to the fact that the least significant bits have changed in the cover image. The PSNR of the proposed method under varying embedding rates are always greater than 40 decibels and that lies in the acceptable range.

6. Conclusion

Security in hybrid cluster cloud environment is an important concern in this paper, which is achieved dynamically by hybrid steganographic model in the private cloud. The issues related to security of images in the cloud is carefully handled by the proposed system using dual-type encryption model. This model performs fast and ensures better security with hybrid blowfish and genetic operator model. The selection of chromosomes plays a major part, which is attained in an optimized way than the other cryptographic algorithm over the cloud environment. From the results, it is seen that the proposed method attains better security than the conventional model and ensures fast processing capability. The risk of providing security over dynamic cluster-based private cloud is attained carefully with better operation, which does not increase much the computational complexity of the cloud system. Further, the

Table 3. Execution time (in seconds) of the proposed method with other conventional methods.

	Adaptive LSB substitution [25]	Adaptive neural networks [26]	Iterative magic matrix encryption algorithm [25]	Proposed
Encryption time	124.54	112.14	107.25	86.012
Decryption time	125.03	112.62	106.24	86.547

Table 4. PSNR of the proposed method with other conventional methods.

Embedding rate	LSB replacement	Adaptive LSB substitution [25]	Adaptive neural networks [26]	Iterative magic matrix encryption algorithm [25]	Proposed method
0.25	54	52.5	50.51	48.54	45
0.5	50	48.21	47.28	44.25	42
0.75	48	47.24	46.85	44.28	40
1	45	44.84	42.32	40.32	38
1.25	44	43.65	41.21	40.57	38.43
1.5	43.7	42.15	40.04	38.65	38.1
1.75	43.65	42.84	39.84	38.54	35.5
2	43.1	42.58	38.62	36.45	35.1

work can be improved with the use of proxy-encryption with the highest entropy and least correlation than this work.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

[1] Khan MA. A survey of security issues for cloud computing. J Netw Comput Appl. 2016;71:11–29.

[2] Armbrust M, Fox A, Griffith R, et al. A view of cloud computing. Commun ACM. 2010;53(4):50–58.

[3] Fogarty K. (2009). Cloud Computing definitions and solutions Available from: http://www.cio.com/article/print/501814, Accessed 01.09.17.

[4] AlZain MA, Pardede E, Soh B, et al. Cloud computing security: from single to multi-clouds. In: System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE; 2012. p. 5490–5499.

[5] Flinders K. (2014). Banks could lower costs with cloud computing, but there are risks too. Available from: http://www.computerweekly.com, Accessed 01.09.17.

[6] Gill PS. Cloud computing and enterprise systems: applications in the auto industry. Int J Technol Knowl Soc. 2013;9(1):25–35.

[7] Toxen B. The NSA and snowden: securing the all-seeing eye. Commun ACM. 2014;57(5):44–51.

[8] Zadiraka VK, Kudin AM. Cloud computing in cryptography and steganography. Cybern Syst Anal. 2013;49(4):584–588.

[9] Cheng H, Li X. Partial encryption of compressed images and videos. IEEE Trans Signal Process. 2000;48(8):2439–2451.

[10] Xiang T, Wong KW, Liao X. Selective image encryption using a spatiotemporal chaotic system. Chaos: Interdiscip J Nonlinear Sci. 2007;17(2):023115.

[11] Podesser M, Schmidt HP, Uhl A. Selective bitplane encryption for secure transmission of image data in mobile environments. In: CD-ROM Proceedings of the 5th IEEE Nordic Signal Processing Symposium. NORSIG; 2002.

[12] Gentry C. Fully homomorphic encryption using ideal lattices. In *STOC*. 2009, May;9(2009):169–178.

[13] Gomathisankaran M, Yuan X, Kamongi P. Ensure privacy and security in the process of medical image analysis. In: Granular Computing (GrC), 2013 IEEE International Conference on. IEEE; 2013. p. 120–125.

[14] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography. Advances in Cryptology—EUROCRYPT'98. 1998;1403:127–144.

[15] Liu Q, Wang G, Wu J. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Inf Sci (Ny). 2014;258:355–370.

[16] Yao ACC. How to generate and exchange secrets. In: Foundations of Computer Science, 1986., 27th Annual Symposium on. IEEE; 1986. p. 162–167.

[17] Bringer J, Chabanne H, Patey A. Privacy-preserving biometric identification using secure multiparty computation: an overview and recent trends. IEEE Signal Process Mag. 2013;30(2):42–52.

[18] Hu N, Sen-ching SC, Nguyen T. Secure image filtering. In: Image Processing, 2006 IEEE International Conference on. IEEE; 2006. p. 1553–1556.

[19] Kester QA, Nana L, Pascu AC. A novel cryptographic encryption technique for securing digital images in the cloud using AES and RGB pixel displacement. In: Modelling Symposium (EMS), 2013 European. IEEE; 2013. p. 293–298.

[20] Song C, Lin X, Shen X. Secure and effective image storage for cloud based e-healthcare systems. In: Global Communications Conference (GLOBECOM), 2013 IEEE. IEEE; 2013. p. 653–658.

[21] Nourian A, Maheswaran M. Privacy aware image template matching in clouds using ambient data. J Supercomput. 2013;66(2):1049–1070.

[22] Murakami K, Hanyu R, Zhao Q, et al. Improvement of security in cloud systems based on steganography. In: Awareness Science and Technology and Ubi-Media Computing (iCAST-UMEDIA), 2013 International Joint Conference on. IEEE; 2013. p. 503–508.

[23] Sharp T. An implementation of key-based digital signal steganography. In: Information hiding. Berlin: Springer; 2001. p. 13–26.

[24] Provos N, Honeyman P. Hide and seek: an introduction to steganography. IEEE Secur Priv. 2003;99(3):32–44.

[25] Muhammad K, Sajjad M, Mehmood I, et al. Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Future Gener Comput Syst. 2018;86:951–960.

[26] El-Emam NN, Al-Diabat M. A novel algorithm for colour image steganography using a new intelligent technique based on three phases. Appl Soft Comput. 2015;37:830–846.