Improved method for image security based on chaotic-shuffle and chaotic-diffusion algorithms

Sanjeev Sharma[1], Tarun Kumar[2], Ravi Dhaundiyal[3], Amit Kumar Mishra[4], Nitin Duklan[5], Ashish Maithani[6]
[1,3,4,5,6]Department of Computer Science & Engineering, Uttaranchal University, India
[2]Department of Computer Science & Engineering, Uttarakhand Technical University, India

Article Info

Article history:

Received Mar 5, 2018
Revised Aug 2, 2018
Accepted Aug 21, 2018

Keywords:

Encrytion algorithms
Grayscale images
Image encryption
Image security
RGB images

ABSTRACT

In this paper, we propose to enhance the security performance of the color image encryption algorithm which depends on multi-chaotic systems. The current cryptosystem utilized a pixel-chaotic-shuffle system to encode images, in which the time of shuffling is autonomous to the plain-image. Thus, it neglects to the picked plaintext and known-plaintext attacks. Also, the statistical features of the cryptosystem are not up to the standard. Along these lines, the security changes are encircled to make the above attacks infeasible and upgrade the statistical features also. It is accomplished by altering the pixel-chaotic-shuffle component and including another pixel-chaotic-diffusion system to it. The keys for diffusion of pixels are extracted from the same chaotic arrangements created in the past stage. The renovation investigations and studies are performed to exhibit that the refreshed version of cryptosystem has better statistical features and invulnerable to the picked plaintext and known plaintext attacks than the current algorithm.

Corresponding Author:

Tarun Kumar,
Department of Computer Science & Engineering,
Uttarakhand Technical University,
Suddhowala, Dehradun, Uttarakhand-248007, India.
Email: taretechcse14@gmail.com

1. INTRODUCTION

These days multimedia information has been moved quickly and comprehensively to the goals through the web into different structures, for example, image, audio, video and text. In digital correspondence over the web, everything is unmistakable and open to each client. In this manner, security of information is a fundamental and vital task [1, 2]. There are three objectives of network or information security, for example, privacy, reliability and accessibility. Privacy implies that information is secure and not accessible to the unapproved individual. Integrity refers to the accuracy of information and availability implies that information is in time access to approved individual. Network security is not adequate for dependable correspondence of information like text, audio, video and digital images [3-5].

There are numerous strategies to secure images including encryption, watermarking, digital watermarking, reversible watermarking, cryptography, steganography and so on. In this paper a survey on encryption, steganography and watermarking has been illustrated. So far, they have proposed a half and half security approach that is a fusion of encryption, steganography and watermarking. Securing the storage and transmission of images is one of the foundations of information security. Correspondence conventions like Secure Sockets Layer (SSL) utilize message authentication codes to ensure the right characters of the sender and beneficiary of information sections over the internet [6-8]. In addition, multimedia substance like audio, images or video can be protest of authentication, integrity and information covering strategies. The two principle ways to deal with authentication on imaging science are watermarking and cryptography [9-11].

The fundamental contrast between the two methods is that watermarking expects to present the mark of the owner without changing the visual impression of the information. On the other hand, encoded images are not clear without a separating step. Most watermark methods and cryptosystems additionally look for information integrity. Image steganography could be viewed as a unique instance of watermarking, where the objective is to cover the information into the image [12-15].

Over the previous decades, research in security has focused on the improvement of algorithms and conventions like encryption, authentication, and integrity of textual data or data with comparable attributes. Huge advances in security particularly, the improvement of deviated cryptographic conventions and the origin of string symmetric ciphers-a lot of security issues still torment systems. For instance, hackers abusing shortcomings in different systems and the utilization of lacking cipher keys create visit news features about broken security systems. Regardless of the news features, such issues have been very much investigated and even illuminated on a fundamental level, subsequently they are not the essential concentrate on this uncommon topic issue. Or maybe, the research articles cover the unsolved issues in image security, which relate reasonably nearly to PC designs [16-18]. The unsolved difficulties emerge from the expanded availability and conveyance of multimedia content over internet administrations, for example, the World Wide Web and their implications for licensed innovation security and copyright issues. A developing number of logical gatherings in software engineering and cryptography have gone up against these difficulties.

Researches are at present taking a shot at issues, for example, visual cryptography, instruments for the integrity of image material, digital marks for multimedia data, and data covering strategies. Data covering has accomplished the most elevated fame, considers the significant requirements for ensuring protected innovation rights on multimedia content like images, video, audio, and others [8, 19]. These requirements demand strong arrangements because of the blast of openly accessible multimedia information and the effortlessness with which this information can be circulated, replicated and changed. Watermarking innovation takes care of these demands and gives a plausible way to deal with ensure against-and demonstrate unlawful replicating and redistribution in the digital world [20-22].

Dissimilar to text messages, the multimedia information including image data has some exceptional qualities like high limit, repetition and high relationship among pixels. Now and again image applications require fulfilling their own needs like continuous transmission and handling [23]. One of the fundamental objectives that must be accomplished among the transmission of information over the network is security.

Cryptography is the strategy that can be utilized for secure transmission of data. This system will make the information to be transmitted into an indiscernible frame by encryption with the goal that unique approved people can accurately improve the information. The security of image can be accomplished by different sorts of encryption plans. Diverse commotion based and non- commotion based algorithms have been proposed. Among this the chaotic based methods are thought to be all the more encouraging. The chaotic image encryption can be created by utilizing properties of chaos including deterministic progression and flighty conduct [24, 25]. There are three sorts of encryption methods to be specific substitution, transposition or permutation and strategies that incorporate both transposition and substitution. Substitution plans change the pixel esteems while permutation conspires simply shuffle the pixel esteems based on the algorithm. Sometimes both the methods are consolidated to enhance security. In an image encryption strategy based on Arnold cat map and Chen's chaotic system is proposed. It blends of three permutation methods is portrayed, in which bit level, pixel level and region level permutations are connected in some request. Image encryption is an upgrade to AES algorithm by including a primary key generator. The technique is commotion based utilizing bit level permutation. Permutation at the bit level changes the position of the pixel as well as adjusts its esteem. Novel image encryption techniques based on add up to shuffling plan is delineated. The mixes of two calculated maps are utilized for enhancing the security of encryption, which utilizes multiple chaotic systems [25, 26].

Digital multimedia is data can be conveyed over the PC networks, which is inclined to the security breaches. The countries dispatch the space missions to get the information about the current components in the space. The countries do not need the information to get spilled. So there must be security component which can guarantee the security of between space transmissions. Under this research we are proposing secure system to secure the images in the between space communications. As we realize that, digital data can be duplicated with no misfortune in quality and substance. This represents a major issue for the insurance of protected innovation privileges of the countries and space offices claim that data. Partial image security is an answer for the issue. It incorporates a mix of steganography, cryptography and pressure. Steganography depends on covering secret message in unsuspected multimedia data and utilized as a part of mystery communication between recognized gatherings. Steganography is a technique for encryption that coverings data among the bits of a cover document, for example, a realistic or an audio record. The procedure replaces unused or unimportant bits with the mystery data. Steganography is not as strong to attacks since the inserted data is defenseless against demolition. Cryptography is the specialty of ensuring information by changing it into a mixed up design called cipher text. Just the individuals who have a secret key can decipher the message into plain text. Encoded messages can some of the time be broken by cryptanalysis, additionally called code-breaking, although current cryptography systems are plans and purposes unbreakable. In software engineering and information hypothesis, data pressure, source coding or bit-rate decrease includes encoding information utilizing less bits than the first portrayal. Method can be either lossy or lossless. Lossless pressure lessens bits by recognizing and wiping out statistical excess. No information is lost in lossless pressure [27]. Lossy pressure diminishes bits by recognizing pointless information and expelling it. The way toward diminishing the span of a data document is prominently alluded to as data pressure, despite the fact that its formal name is source. With the quickly developing network, many individuals use the different applications to exchange digital image data. The greater parts of individuals share their own images with different clients utilizing the social application. Hacking attacks on these applications can make extraordinary misfortunes the client security which can bring down the quantity of active clients and so the business prevalence. Presently clients get to these applications from their convenient gadgets such as advanced mobile phone, tablet, etc.). To reduce the hacking attacks on those web or portable application designs, there is different data security instrument for image, video or text data. These current security components are either utilizing encryption or steganography, or their blends. There is different securable and ideal system of image encryption that can be very much shielded from unapproved. With regards to the image exchanges over the web, image security turns into the real security worry for military, security offices, social or versatile applications. To accomplish the objective of image security, various image security and image preparing algorithms are being used independently or in a mix to give the powerful image security. In any case, these current image security components neglect to give the best image security and once in a while turned out to be brittle or hackable. Image transformation is an extra capacity, which can be connected on the image to bring down their memory measure. The known and prevalent algorithms utilized for the data transformation are DFT, DCT, and DWT and so on [28, 29].

Image exchanges over web or intranet are inclined to hacking. The image exchanged over web or intranet can be hacked by hackers utilizing a few attacks such as the passive attack endeavors to learn or make utilization of information from the system yet does not influence system assets. It is of two sorts like release of message content and traffic examination. An active attack contains some data stream updating that is subdivided into disguise, replay, and modification of messages and refusal of administration. End to end authentication can be likewise used to keep image exchange integrity in place, yet end to end authentication is not conceivable if there should be an occurrence of many image exchanges, on the grounds that numerous server based web administrations like Facebook, WhatsApp, and so forth does not let a client to spare the substance in secure configurations, and does not enable the conclusion to-end authentication based conventions.

This research used the NWPU-RESISC45 dataset [30], which is publicly available benchmark for remote sensing image scene classification produced by the Northwestern Polytechnical University, China. This dataset contains 31,500 images, covering 45 scene classes with 700 images in each class and total 45 scene classes. This study used the NWPU-RESISC45 dataset [30] to perform the experiments. The acquired satellite images are two dimensional rectangle arrays. The components of this array are the pixels, which has a particular intensity value and position coordinates [31].

A simple, rapid and sensitive scheme is proposed [32] for an image block cipher encryption for gray scale images using a different set of secret key and sizes. The swap and dispersion have done without keys and in second phase involving first secret key the image is mixed with chirikov map. Multiple rounds have taken to complete the process. A dividation of blocks of block size 8X8 is done for blended image. To achieve good confusion these blocks are also swapped. For a solid encryption scheme, in each block the pixels transmutation is done with three more secret keys modified logistic map.

The research [33] aims at performance evaluation of Doubly Truncated Generalized Laplace Mixture Model and K Means clustering (DTGLMM-K) for image analysis. This work aims at development of DTGLMM-K algorithm which is suitable for wide variety of applications and data. Performance evaluation of the developed algorithm has been done through various measures like PRI, GCE and VOI.

A novel approach called Wavelet based Least Significant Bit Watermarking (WLSBWM) for high authentication, security and copyright protection proposed [34]. Alphabet Pattern (AP) is applied to generate shuffled image in the first stage and Pell's Cat Map (PCM) is applied for more security from intrusion. PCM used on all 5×5 sub images. Concept of Wevlet is applied to decrease the dimensionality of the image until it equals to the size of the watermark image. In first phase DCT is used and then multilevel DWT is used for reducing up to the size of the watermark image. The water mark image is inserted in LH_n Sub band of the wavelet image using LSB concept.

2. PROPOSED METHOD

The Huang et al. [35] proposed a pixel-chaotic-shuffle component which uses four 3D chaotic systems in particular the Henon map, the Lorenz map, the Chua map and the Rossler map for scrambling color images. The four 3D chaotic systems utilized as a part of the outline are depicted by (1), (2), (3) and (4) in this section. These chaotic systems are iterated and handled to create the shuffling. In pixel-chaotic-shuffle system, the entire thought of encryption of RBG images includes two stages. In the main stage, the bits of binaries of image segment are permuted vertically by performing section savvy ordering and shuffling.

In the second stage, the 8-bits of every pixel of image part are modified on a level plane inside themselves through column shrewd ordering and shuffling. One key weakness of Huang et al. algorithm is that the age of shuffling arrangements is autonomous to the pending plain-image or the cipher-image. As a result, it produces same arrangements for encoding diverse plain-images. Another reason which makes crafted by assailant less demanding is that each color segment of plain-image is prepared independently and autonomously. These inadequacies encourage the cryptanalysts Solak et al. to break their algorithm. We propose security enhancements in Huang et al. algorithm with comparable fundamental portrayal, parameters and capacities utilized. The enhancements are surrounded to preclude the previously mentioned weaknesses of the current strategy. A changed pixel-chaotic-shuffle system is exhibited to make a confidence of twelve shuffling arrangements to the plain-image to be scrambled and the process three segments of color image.

Also, the adjusted pixel-chaotic-shuffle method is added by proposed pixel-chaotic-diffusion system to upgrade the statistical features of refreshed variant. Accordingly, the enhancements make the cryptanalysis, executed, infeasible and additionally enhance the statistical features of cryptosystem.

The plaintext color image $N * 3$ of size$m * n * 3$, is first vectorized utilizing raster-check strategy (in $R \rightarrow G \rightarrow B$ arrange) to get a variety of size$N * 3$, where$N = mn$. The pixel's force esteems are decayed into its paired counterparts of 8-bit configuration to shape a parallel image grid ξ of size$N * 24$. To make the shuffling arrangements subject to plain-image, the aggregate number of 1s in binary color image ξ is ascertained, given it a chance to be Δ. The four parameters NH, NL, NC and NR are assessed based on the estimation of Δ. The four chaotic systems with indicated scratch parameters are iterated for NH, NL, NC and NR times and came about chaotic esteems are disposed of. It is done to accomplish two purposes: to build up a connection between the plain-image and the chaotic groupings or inevitably the shuffling successions and to evacuate the transient impact of the chaotic systems utilized. The future directions of the four systems are exclusively controlled by the parameter Δ, which is particular to the pending plain-image. In this way, it extricates information from the plain-image and uses it to repeat the chaotic systems. Thus, an altogether unique arrangement of successions is produced while scrambling a somewhat extraordinary plain-image. It assumes a key part in overcoming the potential picked plaintext assault and known-plaintext assault. The 24-bits of each line of paired image grid ξ is physically masterminded in a way appeared in Figure 1, to bring the underlying confusion among RGB pixels, let rgb be the network acquired. Thus, building up the confidence of segments on each other, this expands the calculation of cryptanalysis. Along these lines 8-bit pixel of every R, G, B segment that was shuffled separately has been swapped by 24-bit design for each RGB pixel in the refreshed adaptation. The technique is then trailed by segment insightful ordering and shuffling, push shrewd ordering and shuffling and pixel-chaotic-diffusion.

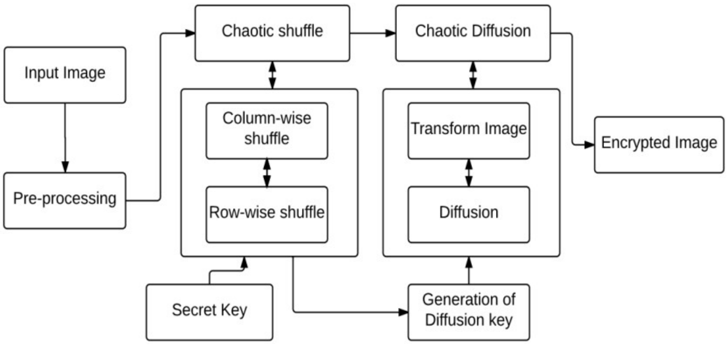

Figure 1. The proposed method

The following twelve chaotic sequences are obtained by applying next mn iterations to each chaotic systems, $X_i(k), \mathrm{Y}_i(k)$ and $Z_i(k)$, where $i = 1,2,3,4$.

$$X_i = \{\mathrm{x}_i(1), \mathrm{x}_i(2), \ldots.., \mathrm{x}_i(\mathrm{mn})\} \tag{1}$$

$$Y_i = \{\mathrm{y}_i(1), \mathrm{y}_i(2), \ldots.., \mathrm{y}_i(\mathrm{mn})\} \tag{2}$$

$$Z_i = \{\mathrm{z}_i(1), \mathrm{z}_i(2), \ldots.., \mathrm{z}_i(\mathrm{mn})\} \tag{3}$$

To improve their stochasticity and randomness, these sequences are preprocessed using following formulation, where $k = 1, 2, \ldots., \mathrm{mn}$

$$\begin{aligned} X_i^{'}(k) &= \{\mathrm{X}_i(\mathrm{k})*10^6 - \mathrm{floor}(\mathrm{X}_i(\mathrm{k})*10^6)\} \\ Y_i^{'}(k) &= \{\mathrm{Y}_i(\mathrm{k})*10^6 - \mathrm{floor}(\mathrm{Y}_i(\mathrm{k})*10^6)\} \\ Z_i^{'}(k) &= \{\mathrm{Z}_i(\mathrm{k})*10^6 - \mathrm{floor}(\mathrm{Z}_i(\mathrm{k})*10^6)\} \end{aligned} \tag{4}$$

3. RESULT AND DISCUSSION

Security attacks are obvious for use in attack investigations, since grayscale images are utilized as a part of executions. The particular region of the mixed image is changed into a white region for damage assault investigation. Thus, the particular region of the mixed image is changed into a dark region for impediment assault investigation. For instance, the extent of the particular region is resolved as 50×50, and the impediment and damage assault investigations utilizing this region are executed to images.

To evaluate the reliability of the proposed technique, security attacks are actualized to one-quarter and half of an image. This methodology is repeated 10 times for each attack inspection and the PSNR esteems are processed. The acquired outcomes from these examinations are appeared in Figure 2 and computed PSNR esteems for both attack investigations are given as normal esteems in Figure 3. The results comes about because of these assault examinations affirm the reliability of the proposed strategy. The recovered image can in any case be resolved to be improved from which image effortlessly, regardless of whether half of this image is destroyed. At the end of the day, when the mixed image is presented to outer attacks, the technique opposes these attacks intensely. Correlation coefficient estimation of image pixels precented in Figure 4.

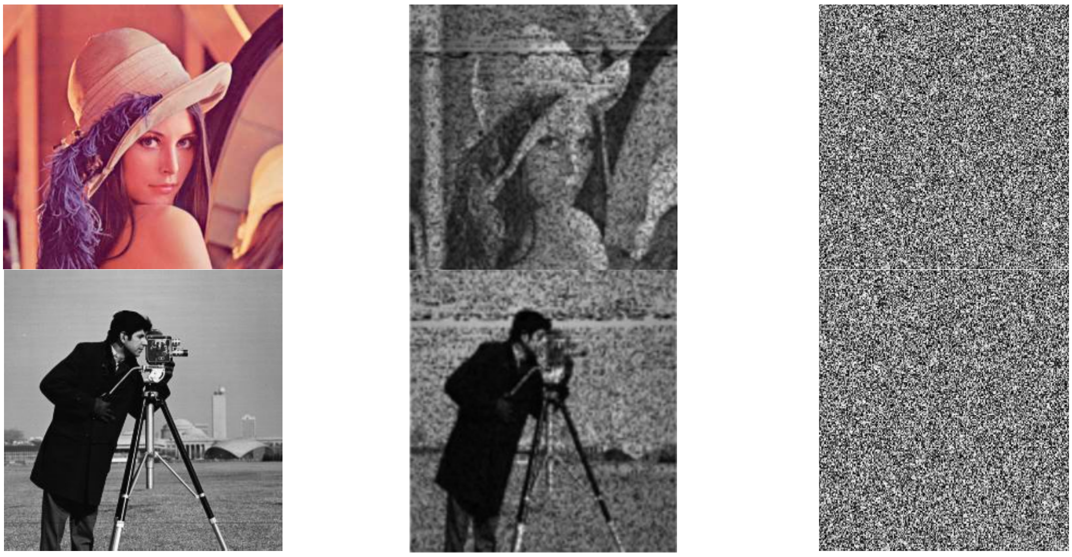

Figure 2. Attack effected images and encryption results from the proposed method

In the proposed method, the statistical properties of color plain-images are enhanced in such a way to the point that jumbled images have great adjust property. To measure the adjust property of images, the mean dimension estimations of plain-image and scrambled images are evaluated and recorded. As can be seen from scores that regardless of how dark estimations of plain-image are disseminated, the mean dimension estimations of encoded images turn out more like 127.5, when contrasted with the current cryptosystem. This demonstrates the enhanced variant doesn't give any information in regards to the conveyance of dimension esteems to the attacker in the encoded images.

The security performance of an encryption method is also quantified through chi-square test. It is a statistical test used to examine the variations of data from the expected value. The acquired outcomes demonstrates a fast in performing encryption and decoding process and in getting the outcomes, yet in addition we should say that diminishing the measure of encoded part influences the relationship between the cipher image and the original image increase.

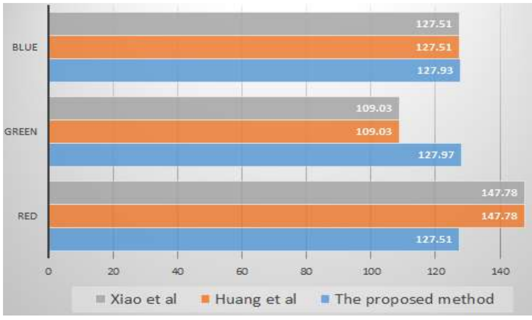

Figure 3. Estimated average image gray value results

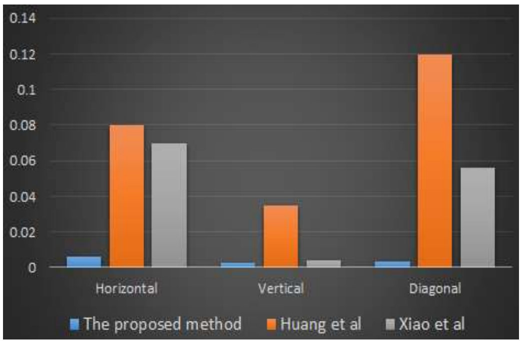

Figure 4. Correlation coefficient estimation of image pixels

4. CONCLUSION AND FUTURE WORK

In this paper an updated version of color image encryption algorithm has been proposed. The weaknesses of existing procedure are wiped out by progressively changing the shuffling successions at whatever point there is a minor change in plain-image. It is accomplished by removing information particular to the pending plain-image and utilizing it to create the shuffling arrangements. The R, G, B parts of image are worked on the whole and conditionally. This ensures the strength of the proposed algorithm against security attacks. The statistical features of the algorithm are additionally enhanced by including a pixel-chaotic-diffusion stage to it, where the diffusion keys are acquired out of the chaotic successions created before. The obtained results demonstrated that the proposed method is extremely sensitive to a slight change in the plain-image. A few other reproduction investigations and similar considerations approve the enhanced security execution of the proposed method. The outcomes got from these analyses demonstrated that this method is very fruitful for grayscale images and can be utilized successfully in any image watermarking and image encryption applications. Besides, as talked about in the past segments, the algorithm can be increased for use in color, high-determination, uproarious, and low-differentiate images.

ACKNOWLEDGEMENTS

The authors cordially thank the Uttaranchal University, Dehradun, INDIA for supporting this work.

REFERENCES

[1] Pfleeger, C.P. and S.L. Pfleeger, "Security in Computing", *Prentice Hall Technical Reference*, 2002.

[2] Kumar, S., et al., "Fast and Efficient Medical Image Compression Using Contourlet Transform", *FEMI-CCT Open Journal of Computer Sciences*, pp. 7-13, 2013.

[3] Krutz, R.L. and R.D. Vines, "Cloud Security: A Comprehensive Guide To Secure Cloud Computing", *Wiley Publishing*, 2010.

[4] Rabbani, M., "JPEG2000: Image Compression Fundamentals, Standards and Practice", *Journal of Electronic Imaging*, vol. 11, pp. 286, 2002.

[5] Singh, V., et al. "3D Reconstruction Of ATFL Ligament Using Ultrasound Images", *5th International Conference onIntelligent and Advanced Systems (ICIAS*), IEEE, 2014.

[6] Joyce, K.E., et al., "A Review of the Status of Satellite Remote Sensing and Image Processing Techniques for Mapping Natural Hazards and Disasters", *Progress in Physical Geography*, vol. 33, pp. 183-207, 2009.

[7] Ford, W. and M.S. Baum, "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption", *Prentice Hall PTR*, 2000.

[8] Singh, V., et al., "Impacting Clinical Evaluation of Anterior Talofibular Ligament Injuries Through Analysis of Ultrasound Image", *Biomedical engineering online*, vol 15, pp. 13, 2016.

[9] Katkovnik, V., K. Egiazarian, and J. Astola,"Local Approximation Techniques in Signal and Image Processing", *SPIE Bellingham*, 2006.

[10] Siponen, M.T. and H. Oinas-Kukkonen, "A Review of Information Security Issues and Respective Research Contributions", *ACM Sigmis Database*, vol 38, pp. 60-80, 2007.

[11] Singh, V., et al., "Computer aided Diagnosis (CAD) Tool for the Analysis of Calcaneofibular Ligament Using Ultrasonographic Images", *ARPN Journal of Engineering and Applied Sciences*, vol 11, pp. 8972-8977, 2016.

[12] Javidi, B., G. Zhang, and J. Li, "Experimental Demonstration of the Random Phase Encoding Technique for Image Encryption and Security Verification", *Optical Engineering*, vol 35, pp. 2506-2513, 1996.

[13] Mellado, D., et al., "A Systematic Review of Security Requirements Engineering", *Computer Standards & Interfaces*, vol 32, pp. 153-165, 2010.

[14] Podilchuk, C.I. and E.J. Delp, "Digital Watermarking: Algorithms and Applications", *IEEE signal processing Magazine*, vol 18, pp. 33-46, 2001.

[15] Anandan, P. and R. Sabeenian, "Image Compression Techniques using Curvelet, Contourlet, Ridgelet and Wavelet Transforms–A Review", *Biometrics and Bioinformatics*, vol 5, pp. 267-270, 2013.

[16] Matoba, O., et al., "Optical Techniques for Information Security", *Proceedings of the IEEE*, vol 97, pp. 1128-1148, 2009.

[17] Cheddad, A., et al., "Digital Image Steganography: Survey and Analysis of Current Methods", *Signal processing*, vol. 90, pp. 727-752, 2010.

[18] Elamvazuthi, I., et al., "Development of an Autonomous Tennis Ball Retriever Robot As an Educational Tool" *Procedia Computer Science*, vol 76, pp. 21-26, 2015.

[19] Coatrieux, G., et al. "Relevance of Watermarking in Medical Imaging",*IEEE EMBS International Conference on Information Technology Applications in Biomedicine*, 2000.

[20] Jaquith, A., "Security Metrics: Replacing Fear, Uncertainty, and Doubt", *Addison-Wesley Professional*,2007.

[21] Gupta, V. and M.A. Barve, "A Review on Image Watermarking and Its Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, pp. 92-97, 2014.

[22] Singh, V., et al., "Clinical Assessment of Injured Ankle ATFL *ligaments based on ultrasound imaging in the athletes",* 6th International Conference on Intelligent and Advanced Systems (ICIAS), IEEE, 2016.

[23] Kumar, M., A. Aggarwal, and A. Garg, "A Review on Various Digital Image Encryption Techniques and Security Criteria", *International Journal of Computer Applications*, vol. 96, 2014.

[24] Furht, B., E. Muharemagic, and D. Socek, "Image Encryption Algorithm", *Multimedia Encryption and Watermarking*, 2005, pp. 79-120.

[25] Ozturk, I. and I. Sogukpinar, "Analysis and Comparison of Image Encryption Algorithm", *International Journal of Information Technology*, vol. 1, pp. 108-111, 2004.

[26] Gao, H., et al., "A New Chaotic Algorithm for Image Encryption", *Chaos, Solitons & Fractals*, vol. 29, pp. 393-399, 2006.

[27] Mao, Y., G. Chen, and S. Lian, "A Novel Fast Image Encryption Scheme based on 3D Chaotic Baker Map" *International Journal of Bifurcation and chaos*, vol. 14, pp. 3613-3624, 2004.

[28] Gao, T. and Z. Chen, "Image Encryption based on a New Total Shuffling Algorithm", *Chaos, solitons & fractals*, vol. 38, pp. 213-220, 2008.

[29] Kwok, H. and W.K. Tang, "A Fast Image Encryption System based on Chaotic Maps with Finite Precision Representation", *Chaos, solitons & fractals*, vol. 32, pp. 1518-1529, 2007.

[30] Cheng, G., J. Han, *and X. Lu, "*Remote Sensing Image Scene Classification: Benchmark and State of the Art*", Proceedings of the IEEE*, 2017.

[31] Khan, M.K., L. Xie, and J. Zhang, "Chaos and NDFT-based Spread Spectrum Concealing of Fingerprint-Biometric Data Into Audio Signal", *Digital Signal Processing*, vol. 20, pp. 179-190, 2010.

[32] Nidhi Sethi, Sandip Vijay, "A New Cryptographic Strategy for Digital Images", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 4, pp. 456-462 June, 2014.

[33] T Jyothirmayi, K Srinivasa Rao, P Srinivasa Rao, Ch Satyanarayana, "Image Segmentation Based on Doubly Truncated Generalized Laplace Mixture Model and K Means Clustering", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, pp. 2188-2196, October 2016.

[34] V. Ashok Kumar, C. Dharmaraj, Ch. Srinivasa Rao, "A Hybrid Digital Watermarking Approach Using Wavelets and LSB", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, pp. 2483-2495, October 2017.

[35] Huang, C. and H. Nien, "Multi Chaotic Systems Based Pixel Shuffle for Image Encryption", *Optics Communications*, vol. 282, pp. 2123-2127, 2009.

BIOGRAPHIES OF AUTHORS

Sanjeev Sharma is the Assistant Professor in Computer Science Department at Uttaranchal University, Dehradun. His areas of research are Malware Forensics and Image Processing.

Tarun Kumar is the Ph.D Scholar in computer science at Uttarkhand Technical University, Dehradun. He is working as research scholar under the guidance of Dr. Parag Jain, Professor *Roorkee Institute of Technology, Roorkee.* His areas of research are Malware Forensics and MobleAdhoc networks.

Ravi Dhaundiyal is the Assistant Professor in Computer Science Department at Uttaranchal University, Dehradun. His areas of research are Security and Image Processing.

Amit Kumar Mishra is the M. Tech Scholar in ISM at Uttaranchal University, Dehradun. His areas of research are Interenet Security and Image Processing.

Nitin Duklan is the Assistant Professor in Computer Application Department at Uttaranchal University, Dehradun. His areas of research are Discrete Strcutures and Algorithms.

Ashish Maithani is the Assistant Professor in Electrical Department at Uttaranchal University, Dehradun. His areas of research are Image Processing, Linear Algebra, and Power Electronics.