International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

A Modified Image Watermarking Method using Logistics and Rsa Algorithm

Anitta Balsalam Vasanthan

Abstract*: In the current era due to the increasing growth of multimedia data it is necessary to protect them, as they are subjected to cyber-attacks like ransomware, trojan, viruses etc. Thiscanaffecttheconfidentialityandintegrityoftheconfidential data transmitted by private and government organizations over the internet. To protect such data digital watermarking is used highlynowadays.Embeddingdataintodigitalsignalslikeimages, audios and videos in the form of digital watermarking copyright information by which the header of data block orsynchronizationoftimeisadaptedtomarkdata.Mostoftheexistin gwatermarking algorithm encrypts the watermark image using RSA, but this is a time-consuming process. Several other existing techniques like Arnold transformation, LSB, DWT etc. fail to address all the security requirements. This paper puts forth a modified watermarking system that uses RSA encryption algorithm and Scrambling Logistic algorithm. In it the watermark image is encrypted by using Logistic and RSA technique is used for encrypting the scrambling parameters. The host image is decomposed by Integer Wavelet Transform (IWT) and SV Decomposition (SVD) and the watermark image is then incorporated into it. This system has a much higher computational efficiency, robustness and embedding capacity compared to the existingtechniques.

***Keywords: Watermarking, IWT, Logistic, RSA*.**

I. INTRODUCTION

Nowadays the increasing use of digital and internet data transfer has led to various problems related to the integrity and legitimacy of the transmitted data. Image processing refers to the process of changing an image into digital form andthencarryingoutafewspecificoperationsonit,whichis done to either modify the image or to take out some informationofusefromit.Inittheinputisgenerallyanimage and output can be an image or some features of that image. Theimageisusuallytransformedintoa2-Dsignalinorderto apply signal processing techniques on it. Image processing tools has led to the development of various image and video applications.

Thought they have the advantage offlexibility, convenienceandcosteffective,theydonotprovidecopyright protectionanddigitalsecurity.Imageprocessingtoolshasled to the development of various image and video applications. Hence nowadays most of the internet users are employing data hiding methods like cryptology, steganography and watermarking.

One of the first and extensively used data hiding methodwas Cryptology. Though encryption is a formal method to make the data in digital form secure, once the data is decrypted aggressively into an understandable form, henceforththe chance of retrieving the data would become higher. In Steganography a confidential message is fixed into a trusted information, thereby making the presence of the confidential messageunknowntooutsiders.Thecoverinformationcanbe of any kind like text, image, audio, video, etc. Images are generally used in the process because they can be implemented easily and are hard tobreak. Watermarking is another most widely used data hiding method. Digital watermarking can be in two domains: frequency(transform)orspatialdomain[1].Inspatialdomain, the pixel intensity value of digital image is modifiedwhereas in frequency domain, the digital image coefficients are modified by adding some extra data. Embedding data in frequencydomainismoreefficientthanthatinspatialdomain as it provides higher resistance to attacks. It can be done by using techniques like SV Decomposition (SVD) [2], DC Transform(DCT)[3]orDWTransform(DWT)[4].Butthey ave a comparatively slower learning rate and poor capacity for computation. A watermarking system must be secured from various security outbreaks. It should also be highly robust and imperceptible to the human eye [5,6]. All the existing watermarking methods carry out the embedding and extraction processes on the plain media. Hence only the original medias owner or a trusted third party should be the embedder of the watermark[7].

Due to the rapid growth of smart brains and attacking tools a single technique may not offer the required safety to the digital data in the present days. Hence a combination of diversepracticesshouldbeusedtothwartthesesafetyissues. In order to get added security, we can combine various encryption techniques like RSA into the watermarking scheme [8]. When put together with RSA the digital data is transformed into a non-intelligible form which can be decrypted into its initial form only by an approved person having the properkey.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Anitta Balsalam Vasanthan, PG Scholar, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore-632014, Tamil Nadu, INDIA.

A. Motivation

Image watermarking is one of the highly researched area nowadays due to the increased use of internet and secret communications through it. Nowadays most of the secret communications make use of watermarking techniques.
The three main requirements of an efficient digital watermarking scheme are robustness, easy extraction of the watermark without affecting the quality of digital adversary. To solve problems like this we came up a new method that increases the security of the watermark and provides higher robustness as compared to the existing techniques. The case-study model consists of four modules: Integer Wavelet Transformation (IWT) [9], Single Value Decomposition (SVD), Chaotic logistic map and RSA process. The methodology overcomes the drawback of existing techniques by the incorporation of IWT and chaotic logistic map for encryption.

B. Contribution

In most of the prevailing watermarking techniques DWT is used to get a sub-band of lower frequency. But in DWT, the inputisgivenasanintegervalue,whiletheoutputisnotinthe form of integers, which causes changes in the original cover image, also data loss in the original image can happen as DWThidesthemessagebyusingfloatingpointvalues.These limitations are avoided by using IWT and also it hides the information without causing distortion. So, IWT is able to give the user a good visual system and also helps to improve the effectiveness of the system. The case-study model technique consists of four modules: Integer Wavelet Transformation (IWT), Single Value Decomposition (SVD), Chaotic logistic map and RSA process. The methodology overcomes the drawback of existing techniques by the incorporationofIWTandchaoticlogisticmapforencryption.

C. Chosen AnalysisModel

Digitalwatermarkinghasrecentlyattractedmanyresearcher s worldwide as they are perceptible only under certain conditions. It is an area of information hiding which hides important data in the raw data thereby protecting it from illegal duplication or distribution. We choose digital watermarking for our analysis due to the current position in playsininformationhidinganddatatransmission.Mostofthe existing systems make use of Arnold, RSA, DWT, DCT etc. to embed data, but these practices are inherent to many drawbacks like embedding time, capacity, efficiency etc. In this paper we put forward a modified watermarking scheme that eliminates theseimperfections.
Theremainingsectionsofthispaperareasfollows:Section2 confers the related work in which a deep analysis of the existing work is done. In Section 3 a case-study model is given.Section4andSection5discussesaboutthemodeland conclusion.

images, and transparency. Visible watermarks can be easily detected by humaneyes,whereasininvisiblewatermarksthewatermarkis imperceptible when implanted into the host image. But most of the existingtechniques
make use of symmetric encryption methods that can be easily attacked by an

II. RELATEDWORKS

Sun et.al [10] performed semi fragile watermarking using SVD. In it SVD is found out to implant the watermark in the host image and then every image blocks singular values are quantized.Itdoesnotguaranteeanyself-recovery.Patraetal. [11] usedtheChineseRemainderTheorem(CRT)topropose a watermarking system that is fragile. The complexity of computationwashighinthistechniquebutthelocalizationof tamper was low. Naik et al. [12] proposed an image cryptosystemforanuncompressedcolorimage.Initsuperior coefficients are selected by using DCT and Arnoldtransform wasusedtoconfusethecoefficientsselected.Inittheentropy valueiscomparativelyhighandalsoAronldislesssecuredur to its small keysize.
Saikrishna et al. implemented a method in which the host imageisseparatedintoblackandwhiteregionsandtwolevels of DWT was used to decompose them [13].Arnold transformationwasusedtoscramblethewatermarkanditwas implantedinsub-bansofthewhitesurfacedarea.Arnoldhasa lower security for its small size of secret key space. As the transformation cycle of Arnold is very short, if attackers perform a minimum number of scramblings continuously, they can get back the initialimage.
To attain a sophisticated level of security, the works by Saha et al. [14] did encryption of the watermark image by using RSA algorithm and Arnold and the host image was decomposed by DCT, but the encryption of image with RSA consumes a lot of time. Hu et al. projected a blind watermarking system built on blocks that is performed on DWT and DCT domain[15]. Quantization Index Modulation (QIM) was performed on DWT-DCT coefficients to reduce the Bit Error Rate in the watermarked image but the time needed for encryption and decryption is very high.
Ansari et al. put forward a multi-purpose watermarking policy.Initthehostimagewaschangedintowaveletdomain byusingDWTandtheoutstandingsingularvaluesofchanged host were modified on the basis of watermarks major components [16]. LSB insertion was done for locating the tempered region and also to provide self-retrieval features to the methodology. Also Artificial Bee Colony (ABC) is employed to increase the strength of imperceptibility. The chief downside of the technique is that stealth (passive or active) affects the presence ofmessage.
Halagowdaetal.[17]proposedahybridencryptiontechnique that provides a highly secure transmission.

In it a fractal-chaos based hybrid method was employed for encryption and decryption. But the method failed to provide alltherequiredsecurityfeaturesandalsoithasahighentropy level. Mood et al. [18] developed a modified and more safe watermarking method that uses Redundant Wavelet Transform (RWT), SVD and Genetic Algorithm (GA).

The scheme provided extraction of feature and optimization property but the PSNR value was veryhigh. To address the above-said drawbacks to lesser the time consumption as well as to progress the watermarks security alongwithguaranteeinghighstrengthLiuetal.putforwarda novel image watermarking system that uses DWT, SVD, LogisticandRSA[19].Initthewatermarkisinitiallyjumbled by Logistic, and the parameters used for scrambling were encryptedbyapplyingRSAandthencommunicatedthrougha network. In the process of watermarking embedding, single level DWT was performed on the host image and a sub-band of lower frequency was then attained. SVD was used to process the sub-band further. By adding the sub-bands singular value and the watermark that has undergone scrambling, a novel singular value was calculated. It is decomposed again to obtain a novel singular value that was usedtorecreateasub-bandoflowerfrequency.InverseDWT wasperformedonthenewsub-bandtogettheimagethathas been watermarked. But in DWT, the input is given as an integer value, whereas the output is not always an integer value,whichcauseschangesintheoriginalcoverimage.The DWT uses floating point values to hide the message, which causes loss of information in the originalimage.

III. CASE-STUDYMODEL

Watermark embedding and extraction are the two main processes in our case-study model. The sender does the watermark processing and embedding and communicates it over the internet. The receiver performs the watermark extraction and recovery.

i. Integer Wavelet Transform(IWT).

The IWT comprises of four levels of sub-bands such as High-Low, Low-Low, Low-High and High-High[20]. We use the Low sub-band as it is alike the original image. The coefficients of IWT are:

$$LL_{i,j} = \left| \frac{Or_{2i,2j} + Or_{2i+1,2j}}{2} \right| \quad (1)$$

$$HL_{i,j} = Or_{2i+1,2j} - Or_{2i,2j} \quad (2)$$

$$LH_{i,j} = Or_{2i,2j+1} - Or_{2i,2j} \quad (3)$$

$$HH_{i,j} = Or_{2i+1,2j+1} - Or_{2i,2j} \quad (4)$$

Where, $1 \le i \le X/2, 1 \le j \le Y/2$ and $\|$ is denoted as floor value, Or istheoriginalimage,Xisdenotedasheightofthepixeland$Y$ the width. Each of the pixel levels are denoted by(i,j).

Integer wavelet transform (IWT) [21] makes use integer coefficients, this evades rounding error, and thereby a good reconstruction can be obtained.

ii. Singular Value Decomposition(SVD).

SVDiscarriedoutonthehostimage[22].Itiswidelyusedin the areas of image and signal processing. The host image is separated into several smaller blocks and singular values are obtained by performing SVD on these blocks. The decomposition formulais:

$$I = U \cdot S \cdot V^T \quad (5)$$

whereIisthe$m \times n$imagematrix,Uisan$m \times m$matrix,Visan $n \times n$matrix,Sisdiagonalmatrixhavingthesizeof I,andTis the coefficient of matrixtransformation.

ThemainadvantagesofusingSVDare:fixedcoefficientsiz e, a change in image values do not change the singular

Here the public key is (e, N) and private key which is kept undisclosedis(d,N).Themessageisencryptedbythesend er using the public key of receiver and then it iscommunicated. The data is decrypted by the receiver using their privatekey.

A. Embeddingphase

The execution steps of message embedding phase are :

Step 1: Pick a scrambling parameter and encrypt it by using RSA algorithm.

Step 2: Apply Logistic algorithm to obtain the scrambled watermark W_d from the gray-scale watermark image W.

Step 3: IWT is used to decompose the host image C into four sub-bands.

Step 4: SVD is done on the LL sub-band, $U_C \cdot S_C \cdot V_C = SVD(LL)$.

Step5:AsingularvalueS$_{new}$isfoundbysummingupS$_C$and the jumbledwatermark along with a scaling factor α,

$$S_{new} = S_C + \alpha \cdot W_d$$

Step 6: Now apply SVD on the newly formed singularvalue,

$$U_W \cdot S_W \cdot V_W = SVD(S_{new})$$

Step 7: LL_{new}, a new coefficient is found,

$$LL_{new} = U_C \cdot S_w \cdot V_C$$

Step 8: Obtain the watermarked image C_W by doing inverse IWT with the new coefficients.

values, and the basic features of an image can be represented by the singular values [23].

iii. Logistic

Logistic map is a 1-D chaotic mapping scheme which is defined by [24,25]:

$$X(k+1) = u * X(k) * [1 - X(k)] \quad (6)$$
$$k = 0,1,\ldots.n$$

Where, and X(k) refers to the variable used for mapping and *u* refers to the system parameter. An m×n image is iterated m ×n times to attain a 1-D sequence. A sequence in the range of (0,255) is obtained by normalizing thissequence.Itisthenconvertedintoa2-Dmatrix,whichis the image matrix that has been encrypted. Here [X (0), u] is thekey.

iv. RSA

It is a public key encryption scheme that uses asymmetric encryption technique [25]. In it the data is protected byusing a pair of keys and it belongs to the block-cipher field [26].It is one among the main functional public-key cryptosystems andisextensivelyusedforsecuredatatransmission[27].The steps for RSA key generationis:

Step1:Chooseanytwolargenumbers*m*andnthatareprime.

Step 2: Find the secret key N and Euler's TotientFunction φ(N) by using:

$$N = m \times n, \emptyset(N) = (m-1) \times (n-1) \quad (7)$$

Step 3: Select a key(for encryption) that satisfies the condition:

$$1 < e < \emptyset(N), \gcd(e, \emptyset(N) = 1 \quad (8)$$

Step 4: Compute the key *d*(for decryption) by using:

$$e \times d = 1 mod \emptyset(N), 0 \leq d \leq N \quad (9)$$

IV. DISCUSSION

In digital era, due to wide use of internet, digital watermarking methods are employed to transmitconfidential data between the users. But many of the prevailing watermarking systems are exposed to attacks by adversaries. Alsotheycancauselossofdata,issuesrelatedtosecurityand are mostly time consuming. To address these issues our systemmakeuseofacombinationofIWT,LogisticandRSA techniques. IWT is used to convert the image chosen as the host and in it the data loss is much lower as compared to the existing DWT is employed [28]. The scrambling parameters areencryptedusingRSA,whichisahighlysecureasymmetric encryptionmethod.Sinceonlythescramblingparameters are encrypted as compared to the whole watermarked image, the systemprovidessecurityandalsoisnottimeconsuming.Thus oursystemremovesthedrawbacksencounteredinmostof the existing watermarking systems and provides an efficient system that is fast and secure at the sametime.

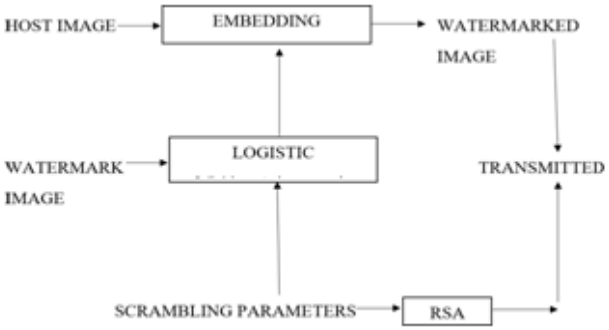

Fig.1 EMBEDDING PHASE.

B. Extractionphase

It is the reverse of the embedding phase. First in order to get thelowfrequencyestimatedcoefficientIWTisappliedtothe watermarked image, which is decomposed once again. The jumbled watermark is found by using the host image and the singular value S_{new} that was formed newly. The scrambling parameterisdecryptedbyusingthereceiversprivatekeyand it is then used to obtain the originalwatermark.

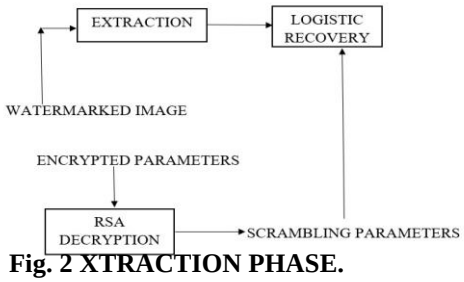

Fig. 2 XTRACTION PHASE.

AUTHOR	METHOD	PROPOSED	CHALLENGES
Saikrishna et al. [4]	Two levels of DWT is employed todecompose the original image and the watermarkedimage, which was jumbledwith Arnold andimplanted into its sub-bans.	Proposed an invisibleand secure logowatermarking usingArnold Transfor-mation.	The original image can be returned once a minimum number of scrambling process is continuously performed by the attackers, that is the conversion cycle of Arnold which is not lengthy.
Liu et al. [8]	Logistic and RSA algorithm was done to watermark image and then it wasincorporated into the sub-band's lower frequency of the host image that was obtained by applying DWT and SVD on it.	Proposed a more secure and robustwatermarking system.	DWT uses floating point to hide the message, which causes data loss in the original image.
Ambedkar et al.[30]	Watermarking is done using DWT and encryption techniques.	Proposed a method that uses DWT and a row-column rotationbased encryption techniqueusing a randomly generatedkey.	The method inherits all the existing drawbacks of DWT.

TABLE 1.

V. CONCLUSION

In this research paper, an effective and improved watermarking technique that is secure, robust and imperceptible has been put forth as a case-study. In it an image in its gray-scale form is set in into the original host image chosen by using the values that are singular in its sub-band of lower frequency. The mixture of a scrambling techniqueandahighlysecureencryptionschemewasusedto increasethesecrecyofthewatermarkingsystem.Thefeatures usedforscramblingcanbestolenwhenthedataistransmitted throughapublicchannel,anasymmetricencryptiontechnique can help guard those parameters form the attack ofmalicious users. In our system we use RSA to encrypt the scrambling parameters, thus making it highly secure. In future work, an effective optimization technique can be used to further increase the efficiency of the models systemsperformance.

REFERENCES

1. Vali, M. H., Aghagolzadeh, A., &Baleghi, Y. (2018). Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition. *Expert Systems with Applications*, *114*,296-312.
2. Abdallah, H. A., Ghazy, R. A., Kasban, H., Faragallah, O. S., Shaalan, A. A., Hadhoud, M. M., ... & El-Samie, F. E. A. (2014). Homomorphic image watermarking with a singular value decomposition algorithm. *Information Processing & Management*, *50*(6),909-923.
3. Laouamer, L., &Tayan, O. (2015). A semi-blind robust DCT watermarkingapproach
4. for sensitive text images.
5. *Arabian Journal forScience*
6. *and Engineering*, *40*(4), 1097-1109.
7. Malonia, M., & Agarwal, S. K. (2016, March). Digital image watermarking using discrete wavelet transform and arithmetic progression technique. In *2016 IEEE Students' Conference on Electrical, Electronics and ComputerScience (SCEECS)* (pp. 1-6).IEEE.
8. Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In *INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005.* (pp. 709-716).IEEE.
9. Haouzia, A., &Noumeir, R. (2008). Methods for image authentication: a survey. *Multimedia tools and applications*, *39*(1), 1-46.
10. Guo, J., Zheng, P., & Huang, J. (2015). Secure watermarking scheme against watermark attacks in the encrypted domain. *Journal of Visual Communication and Image Representation*, *30*, 125-135.
11. Sharma, A., Singh, A. K., &Ghrera, S. P. (2017). Robust and secure multiple watermarking for medical images. *Wireless Personal Communications*, *92*(4), 1611-1624.
12. Agrwal,S.L.,Yadav,A.,Kumar,U.,&Gupta,S.K.(2016, September). Improved invisible watermarking technique using IWT-DCT. In *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 283-285).IEEE.
13. Sun, R., Sun, H., &Yao, T. (2002, August). A SVD-and quantization based semi-fragile watermarking technique for image authentication. In *6th International Conference on Signal Processing, 2002.* (Vol. 2, pp. 1592-1595).IEEE.
14. Patra, B., & Patra, J. C. (2012, November). Crt-based fragile self-recovery watermarking scheme for image authentication and recovery. In *2012 International Symposium on Intelligent Signal Processing and Communications Systems* (pp. 430-435).IEEE.
15. Naik, K., & Pal, A. K. (2014). A Partial Image Cryptosystem Based on Discrete Cosine Transform and Arnold Transform. In *Recent Advances in Information Technology* (pp. 65-73). Springer, NewDelhi.
16. Saikrishna, N., &Resmipriya, M. G. (2016). An invisible logo watermarking using Arnold transform. *Procedia Computer Science*, *93*, 808-815.
17. Saha,B.J.,Pradhan,C.,Kabi,K.K.,&Bisoi,A.K.(2014, March). Robust watermarking technique using Arnold's transformation and RSA in discrete wavelets. In *Information Systems and Computer Networks (ISCON), 2014 International Conference on* (pp. 83-87).IEEE
18. Hu, H. T., & Hsu, L. Y. (2017). Collective blind image watermarking in DWT-DCT domain with adaptive embedding strength governed by quality metrics.*Multimedia Tools and Applications*, *76*(5),6575-6594.
19. Ansari, I. A., & Pant, M. (2017). Multipurpose image watermarkinginthedomainofDWTbasedonSVDandABC. *Pattern Recognition Letters*, *94*,228-236.
20. Halagowda, S. R. M., &Lakshminarayana, S. K. (2017). ImageEncryptionMethodbasedonHybridFractal-Chaos
21. Algorithm. *International Journal of Intelligent Engineering and Systems*, *10*(6), 221-229.
22. Mood, N. N., &Konkula, V. S. (2018). A Novel Image Watermarking Scheme Based on Wavelet Transform and Genetic Algorithm. *International Journal of Intelligent Engineering and Systems*, *11*(3),251-260.
23. Liu, Y., Tang, S., Liu, R., Zhang, L., & Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications*, *97*,95-105.
24. Makbol, N. M., Khoo, B. E., Rassem, T. H., &Loukhaoukha, K. (2017). A new reliable optimized image watermarkingschemebasedontheintegerwaveletransform and singular value decomposition for copyright protection. *Information Sciences*, *417*,381-400.
25. Arsalan, M., Malik, S. A., & Khan, A. (2012). Intelligent reversible watermarking in integer wavelet domain for medical images. *Journal of Systems and Software*, *85*(4), 883-894.
26. Verma, V. S., & Jha, R. K. (2015). An overviewof robust digital image watermarking. *IETE Technical review*, *32*(6), 479-496.
27. Thakkar, F. N., & Srivastava, V. K. (2017). A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. *Multimedia Tools and Applications*, *76*(3),3669-3697.
28. Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. *Image and vision computing*, *24*(9),926-934.
29. Fatema, M., Maheshkar, V., Maheshkar, S., &Agarwal,
30. G. (2018, August). Tamper detection using fragile image watermarking based on chaotic system. In *International Conference on Wireless Intelligent and Distributed EnvironmentforCommunication*(pp.1-11).Springer,Cham.
31. Rojat, A. (2012). Review of cryptanalysis of RSA andits variants by Jason Hinek. *ACM SIGACT News*, *43*(1),16-18.
32. Kishore,P.V.V.,Venkatram,N.,Sarvya,C.,&Reddy,L.
33. S. S. (2014, August). Medical image watermarking using RSA encryption in wavelet domain. In *2014 First International Conference on Networks & Soft Computing (ICNSC2014)* (pp. 258-262). IEEE.
34. Kaur, G., & Verma, S. K. (2018, July). Multi-Level Secured Encryption Technique Using Enhanced Fractal Image Watermarking. In *2018 International Conference on InventiveResearchinComputingApplications(ICIRCA)*(pp. 314-322).IEEE.
35. Singh, S., Singh, R., & Siddiqui, T. J. (2016). Singular value decomposition based image steganography using integer wavelet transform. In *Advances in signal processing and intelligent recognition systems* (pp. 593-601). Springer, Cham.
36. Ambadekar,S.P.,Jain,J.,&Khanapuri,J.(2019).Digital Image Watermarking Through Encryption and DWT for Copyright Protection. In *Recent Trends in Signal and Image Processing* (pp. 187-195). Springer,Singapore.

AUTHORS PROFILE

Anitta Balsalam Vasanthanis currently pursuing her MTech in Computer Science and Engineering(Spec. in Information Security) at VIT University, Vellore, India.