International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

A Novel Method on Enhanced Video Security using Steganography

C.Senthilkumar, K.Gayathri Devi, M.Dhivya, R.Rajkumar

Abstract: ***Security is imperative to individuals' key opportunity. In the course of recent decades with the headway of correspondence innovation the utilization of web has developed amazingly to trade data with no separation bearer. The most recent drama covers the threats against our technology infrastructures. The most challenging issue in the military network is that secure retrieval of confidential data. Information installing is the way toward implanting data in an information source without changing its perceptual quality. Stenography is the method of thrashing a document, message, picture or video surrounded by another record, message, picture or video. In previous methods, usage of image and text as key produces low security and reversible data hiding as algorithm produces less compression ratio. In our paper we proposed a novel method for increasing the video security by using One Time Password (OTP) and voice key as password and improving compression rate by using Blind detection algorithm. The uses of blind detection algorithm includes greater computational accuracy, high flexibility and deliver faster execution by an estimated high PSNR value .In addition, this paper also includes compressing image, audio and video files and embedding into a single video.***

Keywords: Security, Steganography, Data Embedding, Compression ratio, PSNR, Blind Detection Algorithm

I. INTRODUCTION

As of now, web and computerized media are getting increasingly more prominence. In this way, necessity of secure transmission of information additionally expanded [1],[5]. Therefore different great systems are proposed and right now taken into training. Right now, utilize the Steganography [3] process for the protected information transmission from the sender to collector through the web.
Content, picture, sound, and video can be spoken to as computerized information. The blast of Internet applications drives individuals into the computerized world, and correspondence through advanced information becomes intermittent [2]. Be that as it may, new issues additionally emerge and have been investigated, for example, information security in computerized interchanges, copyright insurance of digitized properties [4],[6],[7] imperceptible correspondence through advanced media, and so on..

Manuscript received on April 02, 2020.
Revised Manuscript received on April 20, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
Dr.C.Senthilkumar*, Assistant professor - ECE, Dr.N.G.P. Institute of Technology, Coimbatore, India. Email: senthilkumarc@drngpit.ac.in
Dr.K.Gayathri Devi, Professor - ECE, Dr.N.G.P.Institute of Technology, Coimbatore, India. Email: gayathridevi@drngpit.ac.in
Dr.M.Dhivya, Associate Professor - ECE, New Horizon College of Engineering, Bengaluru, India. Email: dhivyam@newhorizonindia.edu
Mr.R.Rajkumar, Assistant professor - ECE, Dr.N.G.P.Institute of Technology, Coimbatore, India. Email: rajkumar.r@drngpit.ac.in

Steganography is the craft of concealing data in manners that forestall the discovery of covering up [10],[11]message though cryptographic systems attempt to hide the substance of a message. In Steganography, the object of correspondence is the shrouded message and the spread information is just the methods for sending it. Mystery data just as spread information can be any media [8],[9] information like content, picture, sound, video and so on [18],[20]. The target of this work is to build up a Compressed Video Steganographic Scheme[13] that can give provable security high figuring speed, that insert mystery messages into pictures without delivering observable changes. Here we are installing information in video outlines. A video can be seen as an arrangement of still pictures. Information implanting [16] in recordings appears to be fundamentally the same as pictures. Be that as it may, there are numerous contrasts between information covering up in pictures and recordings, where the primary significant distinction is the size of the host media. Since recordings contain more example number of pixels or the quantity of change space coefficients, a video has higher limit than a despite everything picture and more information can be inserted in the video. Likewise, there are a few attributes in recordings which can't be found in pictures as perceptual excess in recordings is because of their transient highlights. Here information concealing tasks are executed totally in the packed domain [16],[14],[12].

II. REVERSIBLE DATA HIDING

The histogram means graphical interpretation of the dissemination of numerical information. It is a measure of the likelihood dissemination of a continual variable and it is first used by Karl Pearson [5]. The development of a histogram, the underlying advance is to detach the entire extent of characteristics into a movement of intervals and consequently check what quantities of characteristics fall into each break. The chart bars are typically demonstrated as succeeding, non-covering between times of a variable [14],[15],[19]. The intervals will be neighboring, and are generally comparing size. In the event that the holders are of proportionate size, a square shape is lift up over the compartment with height relating to the repeat, the amount of cases in every canister. When in doubt, regardless, compartments need not be of identical width; taking everything into account, the raised square shape has zone relating to the repeat of cases in the container the vertical rotate isn't repeat yet thickness the amount of cases per unit of the variable fair and square axis[17],[12]. A histogram may in like manner be institutionalized indicating relative frequencies. It by then shows the degree of cases that fall into all of a couple of classes, with the aggregate of the statures ascending to 1.Examples of variable holder width are appeared on Census organization data underneath.

As the neighboring compartments leave no gaps, the square states of a histogram reach each other to show that the main factor is continuous[11],[22].

Histograms give the thickness of the essential dissemination of the data, and normally for thickness estimation: surveying the probability thickness limit of the fundamental variable.

The total zone of a histogram used for probability thickness is continually institutionalized to 1. If the length of the between times on the x-center point are all of the 1, by then a histogram is undefined from a relative repeat plot.

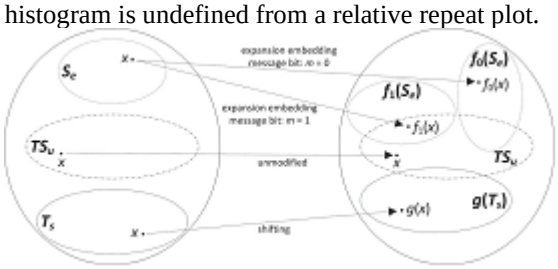


Fig. 1. Illustration of the data embedding procedure by using shifting and embedding functions

This paper will propose a way to deal with improve the exhibition of clinical picture pressure while fulfilling both the clinical group who need to utilize it, and the lawful group who need to protect the emergency clinic against any misbehavior coming about because of misdiagnosis attributable to flawed pressure of clinical images[13]. The improved pressure execution will be practiced by utilizing clinically pertinent locales as characterized by physicians [1].

A. Cumulative histogram

A complete histogram is a mapping that counts the absolute number of discernments in the aggregate of the repositories up to the predefined compartment. That is, the consolidated histogram Mi of histogram m_j is portrayed as:

$$M_i = \sum_{j=1}^{i} m_j. \qquad (1)$$

Sturge's formula

Sturge's formula is gotten from a binomial conveyance and verifiably accepts a roughly typical dissemination

$$k = \lceil \log_2 n + 1 \rceil \qquad (2)$$

It unquestionably assembles the holder sizes regarding the extent of the data and can perform ineffectually if n < 30, in light of the fact that the amount of canisters will be minimal under seven and unlikely to show slants in the data. It may in like manner perform insufficiently if the data are not customarily dispersed.

Doane's formula

Doane's recipe is a difference in Sturges condition which attempts to improve its show with non-customary data.

$$k = 1 + \log_2(n) + \log_2\left(1 + \frac{|g_1|}{\sigma_{g_1}}\right) \qquad (3)$$

B. Patch-based Algorithms

Surface union is the procedure of algorithmically developing an enormous advanced picture from a little computerized test picture by exploiting its basic substance. It is an object of research in PC designs and is utilized in numerous fields, among others advanced picture altering, 3D PC illustrations and after creation of films [4],[21] .

Surface is an uncertain word and with regards to surface combination may have one of the accompanying implications. In like manner discourse, "surface" is utilized as an equivalent word for "surface structure". Surface has been depicted by five distinct properties in the brain science of recognition: coarseness, differentiate, directionality, line-similarity and roughness [7],[21]. In 3D PC designs, a surface is an advanced picture applied to the outside of a three-dimensional model by surface mapping to give the model a progressively sensible appearance. Regularly, the picture is a photo of a "genuine" surface, for example, wood grain. In picture preparing, each computerized picture made out of rehashed components is known as a "surface." For instance, see the pictures beneath. The yield ought to be as comparative as conceivable to the example. The yield must not have obvious relics, for example, creases, squares and misfitting edges.

(1)

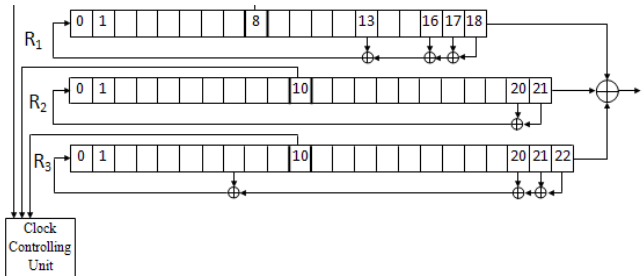


Fig. 2. A Stream Cipher Symmetric Key

III. PROPOSED METHOD

A. Stream-cipher algorithm

A stream figure is a symmetric key figure where plaintext digits are gotten together with a pseudorandom figure digit stream (key stream) [16]. In a stream figure each plaintext digit is encoded one by one with the contrasting digit of the key stream, to give a digit of the figure content stream. Since encryption of each digit is dependent on the current state of the figure, so it is in any case called state figure. The pseudorandom key stream is ordinarily created successively from an unpredictable seed regard using electronic move registers. The seed regard fills in as the cryptographic key for deciphering the figure content stream. Stream figures address a substitute method to manage symmetric encryption from square figures. Square figures chip away at huge squares of digits with a fixed, unvarying change. This separation isn't for each situation self-evident: in specific strategies for action, a square figure rough is used with the goal that it shows sufficiently as a stream figure. Stream figures customarily execute at a higher speed than square figures and have lower hardware unconventionality. In any case, stream figures can be weak to real security issues at whatever point used erroneously (see stream figure attacks); explicitly, a comparable starting state (seed) ought to never be used twice. Stream figures can be seen as approximating the activity of a demonstrated unbreakable figure, the one-time cushion (OTP), now and then known as the Vernam figure. A one-time cushion utilizes a key stream of totally irregular digits. A key stream is connected with the plaintext digits to frame the figure content.

A stream figure uses a significantly more diminutive and logically invaluable key, for instance, 128 bits. Taking into account this key, it creates a pseudorandom key stream which can be gotten together with the plaintext digits thusly to the one-time pad. In any case, this incorporates some critical entanglements. The key stream is by and by pseudorandom as isn't generally sporadic. The check of security related with the one-time pad never again holds. It is truly possible for a stream figure to be absolutely unbound.

In a synchronous stream figure a flood of pseudo-subjective digits is made uninhibitedly of the plaintext and figure texts, and a short time later got together with the plaintext (to scramble) or the figure content (to unscramble). In the most notable structure, twofold digits are used (bits), and the key stream is gotten together with the plaintext using the specific or movement (XOR). This is named a twofold included substance stream figure.

Stream Cipher Algorithm

Step 1: Load the plain video.
Step 2: Transform the original video column digit and to store them in x
Step 3: Find length of the image (N)
Step 4: For i=1: N
Step 5: Generate key stream using below equation Zi =f(ui)
Step 6: End
Step 7: for i= 1 : N
Step 8: Calculate the cipher video digit using relation y(i)=XOR(xi,z(i))
Step 9: End
Step 10: Sent the cipher video digit.

Key stream algorithm

Step 1: To read N, length of y
Step 2: To introduce the secret key, the value of initialization of 13 registers.
Step 3: For t=1: N
Step 4: To generate the output of S1(t), S2(t),……s13(t)
Step 5: End
Step 6: For t=1: N
Step 7: To generate the key stream Z(t)=f(S1(t),s2(t),……s13(t))
Step 8: End

B. LSB Technique

In enlisting, the least basic piece (LSB) is the bit position in a twofold entire number giving the units regard, that is, choosing if the number is even or odd. The LSB is a portion of the time insinuated as the right-most piece, due to the show in positional documentation of forming less tremendous digits further to the other side. It is for all intents and purposes equal to the least basic digit of a decimal entire number, which is the digit during the ones (right-most) position. It is entirely expected to relegate each piece a position number, running from zero to N-1, where N is the quantity of bits in the parallel portrayal utilized. Typically, this is just the example for the comparing bit weight in base-2 Although a couple of CPU makers dole out piece numbers the contrary way (which isn't equivalent to various endianness), the term least critical piece itself stays unambiguous as an assumed name for the unit bit. By expansion, the least critical bits (plural) are the bits of the number nearest to, and including, the LSB.

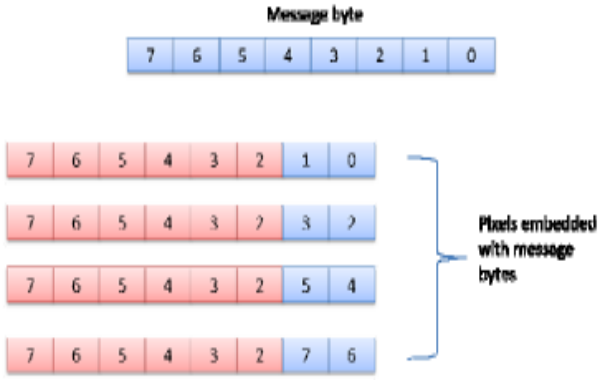


Fig. 3. Least significant bit Technique

The least basic bits have the important property of changing rapidly if the number changes even fairly. For example, if 1 (matched 00000001) is added to 3 (equal 00000011), the result will be 4 (twofold 00000100) and three of the least basic bits will change (011 to 100). Then again, the three most gigantic bits (MSBs) stay unaltered (000 to 000).

Figuring adventures for LSB system:

Each pixel (8 Bits) is hided in 8 pixels of video diagram (1 bit of source picture replaces LSB if 1 pixels in target plot). In case picture size is m1*n1 and packaging size if m2*n2, Then number of pixels in a solitary section of 1 edge that can be hided are given by Y=n2/8 pixels, Number of packaging that can be hided in a videoStep 1. X=(n1/n2)*8

Step 2. For i=1 to x // No of frames.
Step 3. For j=1 to m //No of rows in image.
Step 4. For k=1 to y // No of Columns that can be hided in one frame read bits of pixels.
Step 5. Write bits in LSB if frame pixel
Step 6. End

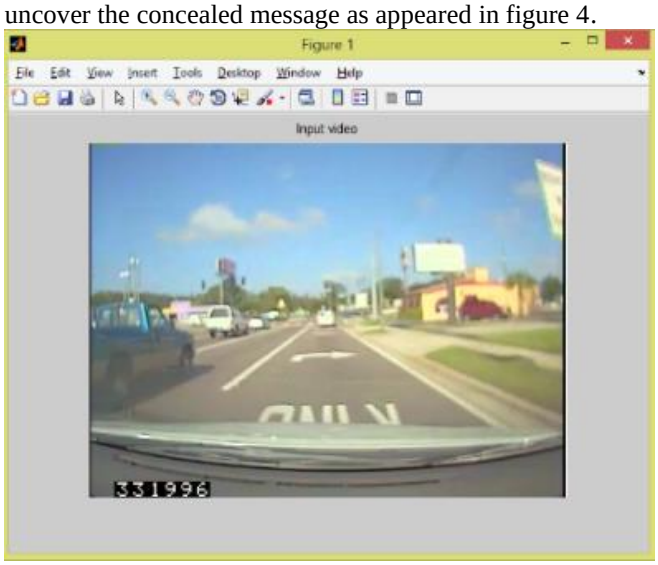
C. Blind Detection Algorithm

Blind source detachment, is the division of a lot of source signals from a lot of blended signs, without the guide of data (or with almost no data) about the source signals or the blending procedure. This issue is when all is said in done profoundly underdetermined, however helpful arrangements can be inferred under an amazing assortment of conditions. A great part of the early writing right now on the division of fleeting signs, for example, sound. Be that as it may, dazzle signal detachment is presently routinely performed on multidimensional information, for example, pictures and tensors, which may include no time measurement at all.
In one methodology, exemplified by head and autonomous part investigation, one looks for source flags that are negligibly related or maximally free in a probabilistic or data theoretic sense. A subsequent methodology, exemplified by nonnegative lattice factorization, is to force auxiliary limitations on the source signals.
Algorithm steps for decryption:
Step 1: Load cipher video digit Y
Step 2: Find length of Y (N)

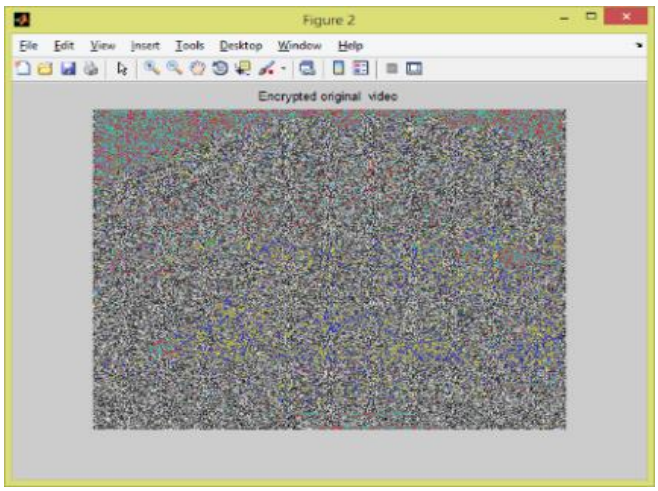
Step 3: For i=1: N
Step 4: To generate the key stream Zi
Step 5: End
Step 6: for i=1: N
Step 7: Calculate the decipher video digit using relation x(i)=XOR(y(i),Z(i))
Step 8: End
Step 9: To put the decipher video x in the form of image of n*m pixels and to store in x

IV. RESULTS AND DISCUSSION

Right now implant the unknown picture, document, video into a solitary video utilizing LSB procedure. Encryption is finished with the assistance of Stream figure and Decryption is finished utilizing Blind discovery calculation. With this task we can shroud an Image, File Video into a spread Video and just when the voice matches with the database it will uncover the concealed message as appeared in figure 4.

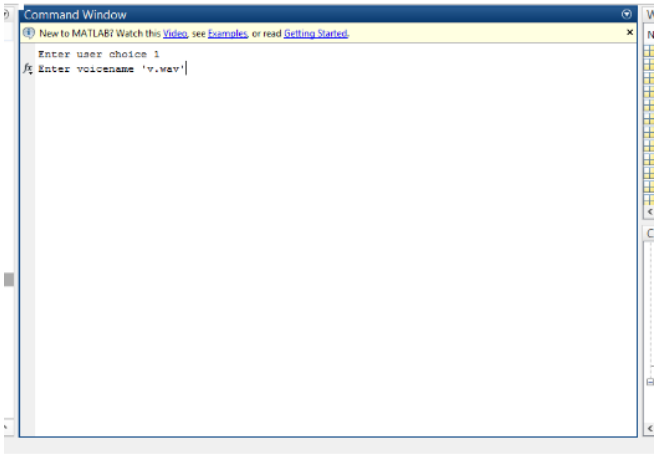


(a) Input Video

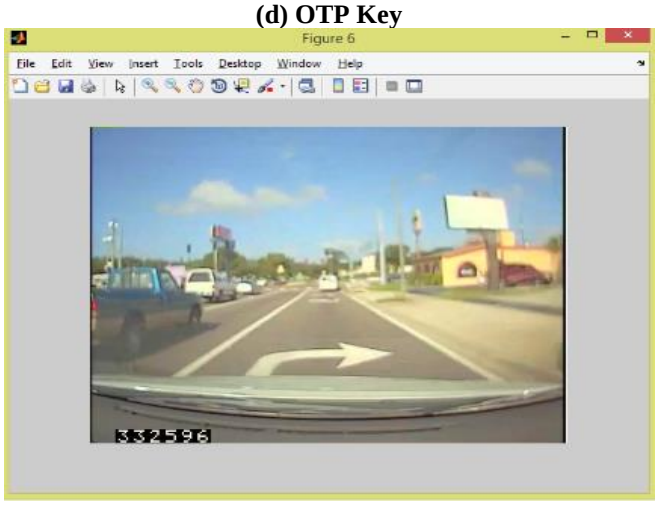


(b) Cover Video

(c) Message Video



(d) OTP Key



(e) Hidden Message Video

V. CONCLUSION

This technique has low multifaceted nature and it is anything but difficult to execute. The trial recreation results on installing picture, video, and record into a solitary spread video. Right now, information concealing technique by utilizing Single piece, no good, three piece LSB substitution and Advanced Encryption Standard. Calculation is performed.

They are ascertaining PSNR and BPP. Right now is diminished when number of LSB substation bit expanded. With the goal that programmers can only with significant effort hack significant data and security is adequate to quit hacking. The outcome examine the connection coefficient has the worth r=1 if there isn't contrast in the first picture. Right now Autocorrelation between unique picture and encoded picture for various casing (Images).They discover no connection between these. Voice is utilized as a mystery key which matches with the key in database. So programmers can only with significant effort hack significant data and security is adequate to quit hacking.

REFERENCES

1. Felix krahmer, rachel ward,2014. Stable and Robust Sampling Strategies for Compressive Imaging,*IEEE Transactions on image processing*, vol. 23, no. 2, February 2014.
2. V. V. Sunil Kumar, M. Indra Sena Reddy,2012. Image Compression Techniques by using Wavelet Transform, *Journal of Information Engineering and Applications*, ISSN 2224-5782, Vol 2, No.5, 2012.
3. Christos Chrysafis, Antonio Ortega,2000. Line-Based, Reduced Memory, Wavelet Image Compression, *IEEE Transactions on image processing*, vol. 9, no. 3, march 2000.
4. J. M. Shapiro,1993. Embedded imaging coding using zero trees of wavelet coefficients, *IEEE Trans. Signal Processing*, vol. 41, pp. 3445–3462, Dec. 1993.
5. Zixiang Xiong, Kannan Ramchandran, Michael T.Orchard, and Ya-Qin Zhang,1999. A Comparative Study of DCT and Wavelet-Based Image Coding, *IEEE Transactions on circuitsand systems for video technology*, vol. 9, no. 5, August 1999.
6. Othman Omran Khalifa,2003. Review of wavelet theory and its Application to Image data Compression, *IIUM Engineering Journal*, Vol. 4, No. 1, 2003.
7. 7. Thomas Meier, King N. Ngan, Gregory Crebbin,1999.Reduction of Blocking Artifact in Image and Video Coding, *IEEE Transactions on circuits and systems for video Technology*, vol. 9, no. 3, April 1999.
8. T. Jarske, P. Haavisto, and I. Def´ee,1994 "Post-filtering methods for reducing blocking effects from coded images, "*IEEE Trans.Consumer Electron*.,vol. 40, pp. 521–526, Aug. 1994.
9. S. Grace Chang,, Bin Yu, Senior Member, Martin Vetterli,2000. Spatially Adaptive Wavelet Thresholding with Context Modeling for Image Denoising, *IEEE Transactions on image processing*, vol. 9, no. 9, September, 2000.
10. I. M. Johnstone and B.W. Silverman,1997. "Wavelet threshold estimators for data with correlated noise," *J. R. Statist. Soc*., ser. B, vol. 59, 1997.
11. Y. Yoo, A. Ortega, and B. Yu,1999 "Image subband coding using Context based classification and adaptive quantization," *IEEE Trans. Image Processing*, vol. 8, pp. 1702–1715, Dec. 1999.
12. Detlev Marpe, Gabi Blättermann, Jens Ricke, and Peter Maaß,2000. A Two-Layered Wavelet-Based Algorithm for Efficient Lossless and Lossy Image Compression,*IEEE Transactions on circuits and systems for video technology*, vol. 10, no. 7, October 2000.
13. Michael B. Martin, Amy E. Bell,2001 New Image Compression Techniques Using Multiwavelets and Multiwavelet Packets, *IEEE Transactions on image processing*, vol. 10, no. 4, April 2001.
14. Aaron T. Deever, Sheila S. Hemami, 2003. Efficient Signal Coding and Estimation of Zero-Quantized Co-efficients in Embedded Wavelet Image Codecs, *IEEE Transactions on imageprocessing*, vol. 12, no. 4, April 2003.
15. B. J. Kim, Z. X. Xiong, andW. A.Pearlman, 2000 "Lowbit-rate scalable video coding with 3-D set Partitioning in hierarchical trees (3-D SPIHT), *IEEE Trans. Circuits. Syst. Video Technol.*, vol. 10, no. 8, pp. 1374–1387, Dec.2000.
16. C. Bajaj, I. Ihm, and S. Park, 2001. "3D RGB image Compression for Interactive applications," *ACM Trans. Graph.*, vol. 20, pp. 10–38, 2001.
17. B. Usevitch,2001. "A tutorial on modern lossy wavelet Image compression: Foundations of jpeg 2000," *IEEE Signal Process.Mag*., vol. 18, no. 5, pp. 22–35, Sep.2001.
18. R. DeVore, B. Jawarth, and B. Lucier, "Image compression through wavelet Transform coding," IEEE Trans. Inform.Theory, vol. 38, pp. 719–746, Mar. 1992.
19. W. B. Pennebaker and J. L. Mitchell, JPEG Still Image Compression Std. New York: Van Nostrand, 1993.
20. M.A. Raja, C. Senthilkumar, B. Arunadevi and P.Divya, 2016. "A Region-based Approach on Segmentation of Medical Image Compression", *International Journal of Printing, Packaging and Allied Sciences*, Vol.04, Dec 2016.
21. Senthilkumar, C., & Gnanamurthy, R. K. (2014). A Performance Analysis of EZW, SPIHT Wavelet Based Compressed Images. *Asian Journal of Information Technology*, 13(11), 684-688.
22. 22. Senthilkumar, C., and R. K. Gnanamurthy. "A Fuzzy clustering based MRI brain image segmentation using back propagation neural networks." *Cluster Computing* 22.5 (2019): 12305-12312.

AUTHORS PROFILE

Dr.C.Senthilkumar received B.E.(ECE) from Bharathiyar University in 2002 and M.E. Applied Electronics in 2008 and Ph.D from Anna university 2019. He has published 8 papers in International journal and 3 papers in National journals and 6 papers in International conferences and currently working as Associate Professor in Dr.N.G.P.Institute of Technology, Coimbatore. He has 16 years of teaching experience and his research interests include Medical image processing, Communications, Pattern recognition and image compression.

.

Dr.K. Gayathri Devi, with 20 years experience working as a Professor in the Department of Electronics and Communication Engineering Dr. N.G.P Institute of Technology, Tamil Nadu, India. She received her B.E. degree in ECE from Coimbatore Institute of Technology (1998), and M.E degree from Dr.Mahalingam College of Engineering and Technology, (2005) and Ph.D in Medical Image Processing (2016) under the affiliation of Anna University, Chennai. She has received Ph.D Guide ship Recognition under the affiliation of Anna University Chennai, in Information and Communication Engineering in the year Jan 2016. She has published papers in national and international Journals, and Conferences. She has Published Patents. She is the reviewer of many SCI and Scopus indexed journals. She has received many proficiency awards, grants and topper in NPTEL online certification examination. She is the Life member in ISTE, International association of Engineers and Institute of Research Engineers and Doctors. Her research interests include Medical Image Processing, Internet of Things, and Artificial Intelligence and Embedded systems.

Dr.M.Dhivya completed her B.E., M.E. and Ph.D. Degree in Electrical and Electronics Specialization. She has 11 years of teaching integrated Research Experience. She has organized more than 30 National Level Symposia/workshop/Conferences and workshops. She has authored and co-authored 40 research papers to her credit. She has guided 40 UG & PG Projects. Her research interests are Embedded and Real Time systems, Optimization techniques and new computational paradigms.

Rajkumar Ramasamy obtained is B.E.degree in Electronics and Communication Engineering and his masters in Communication Systems from Kumaraguru College of Technology, Coimbatore in 2010. He is currently working as Assistant Professor in Department of ECE, Dr.N.G.P institute of Technology, Tamilnadu, India. His interests are in the fields of Image processing, Information security, wireless communication and networking.