International Journal of Recent Trends in Engineering & Research
ISSN (ONLINE) : 2455 – 1457
IMPACT FACTOR : 4.101

ICNSCET20- International Conference on New Scientific Creations in Engineering and Technology

EFFICIENT DATA HIDING WITH COMPRESSION AND EXENCRYPTION FOR SECURE SECRET SHARING

DATA HIDING

Mrs.P.Usha Rani[1] (Assistant professor),
Computer Science and Engineering,Kurinji College of Engineering and Technology
P.Angalaparameswari[2]-ME-Final Year,
Computer Science and Enginnering,Kurinji College of Engineering and Technology

Abstract— Information/data hiding is a mechanism which ensures that the presence of the secret data remains undetected. Two types of data hiding techniques are most popular, they are cryptography and steganography. Where cryptography is science of writing secret code and steganography is art and science of hiding the secret code. In cryptography data is converted to unreadable form, so that unauthorized users cannot access the secret data. Steganography process hides message into cover file and forms a stego file. In image steganography there is a need of method which will increase the security, reduce the distortion in the stego file and recovers the data without any loss. In the era of multimedia and internet there is need of reducing time for transmission. The main objective of this project is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. The secret text was hidden within the QR image. Then QR image can be hidden within secret image. The secret image can be obtained by super imposing the two shares. Conventional k out of n visual cryptography scheme is used to encrypt a single image into n shares. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. A text is written and hidden inside an image. LSB method is used for this purpose. Now the image is splitted into shares. Each share is encrypted using XOR method. The proposed method is n out of n multi secret sharing scheme. Transmission of multiple secret images simultaneously is achieved through this proposed work. The secret image can be revealed only when all the n shares are received by the receiver and decrypted. At the receiver end, the hidden data is extracted from the recovered image.

Keywords

Revresible data hiding,Encryption RDH,Steganography,Scalable compression,Decryption

I. INTRODUCTION

1.1 DOMAIN INTRODUCTION

Steganography s the practice of hiding secret messages (hidden text) within every day, seemingly innocuous objects (cover text) to produce a stego text. The recipient of a stego text can use his knowledge of the particular method of steganography employed to recover the hidden text from the stego text. The goal of steganography is to allow parties to converse covertly in such a way that an attacker cannot tell whether or not there is hidden meaning to their conversation. This sets steganography apart from cryptography which, although providing for private communication, can arouse suspicion based solely on the fact that it is being used.

Modern steganography was characterized by G J Simmons when he stated the problem in terms of prisoners attempting to communicate covertly in the presence of a warden. Alice and Bob, prisoners, are allowed to communicate, but their channel is through the warden, Ward. Alice wishes to pass secret messages to Bob in such a way that Ward can determine neither the contents of the secret messages, nor even that secret messages are being passed.

In modern times, this problem can be observed in national intelligence agencies attempting to detect public yet covert communication between terrorists, or communication between citizens in oppressive states which have outlawed cryptography

II. FORMATTING YOUR PAPER

Title: Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation
Author: Jiantao Zhou, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au and Yuan Yan Tang

Proposed an encrypted-domain RIDH scheme by specifically taking the above-mentioned design preferences into consideration. The proposed technique embeds message through a public key modulation mechanism and performs data extraction by exploiting the statistical distinguishability of encrypted and nonencrypted image blocks. Since the decoding of the message bits and the original image is tied together, our proposed technique belongs to the category of nonseparable RIDH solutions. Compared with the state-of-the-art methods, the proposed approach provides higher embedding capacity and is able to achieve perfect reconstruction of the original image as well as the embedded message bits. Compared with the original unencrypted block, the pixels in the encrypted block tend to have a much more uniform distribution. This motivates us to introduce the local entropy into the feature vector to capture such distinctive characteristics. However, we need to be cautious when calculating the entropy values because the number of available samples in a block would be quite limited, resulting in estimation bias, especially when the block size is small. Instead of considering dedicated encryption algorithms tailored to the scenario of encrypted-domain data hiding, we here stick to the conventional stream cipher applied in the standard format. That is, the ciphertext is generated by bitwise XORing the plaintext with the key stream. If not otherwise specified, the widely used stream cipher AES in the CTR mode (AES-CTR) is assumed. The resulting data hiding paradigm over encrypted domain could be more practically useful because of two reasons.

Merits: Enabling us to jointly decode the embedded message and the original image signal perfectly.
Demerits: The embedding capacity of this type of method is rather limited

Title: Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography
Authors: Monika Bartwal, Dr. Rajendra Bharti

In an image by using the redundancy used a key of reversible data embedding for finding an embedding area. To enlarge the other space the current techniques decrease the redundancy by the execution of pixel value calculation and make use of image histogram. The modern techniques show unlimited embedding volume without severely demeaning the visual excellence of embedded

consequence. The first step is image division, the innovative uncompressed image is separated into two fragments A and B; and monitored through the LSBs. A is reversibly embedded into B, using self-reversible inserting and reversible data hiding technique. LSBs of A can be used to put up extra data. Afterward self embedded data reorganized the encodes image using stream cipher. The values are 0 to 255 and signified by 8 bits. Afterward the encryption process, the data hider put up the encoded image, and insert a limited data into it. The data hider can´t change the original image and only can manage the access to the embedded data. The data mining and data extraction entirely differs from image decryption. Two different case are taking to show.

Merits

It produces individually advanced embedded quality of images provided with a same embedding capacity.

Demerits

The proposed technique cannot be verified on various attacks.

Title: Improved Reversible Data Hiding in Encrypted Images Based on Reserving Room after Encryption and Pixel Prediction

Authors: Ioan Catalin Dragoi, Henri-George Coanda and Dinu Coltuc

RDH scheme for encrypted images based on dividing the encrypted image into blocks and embedding a bit in each block by flipping the 3 least significant bit values of half the pixels from the block. At the decoding stage, the correlation between the decrypted pixels of each block is used to detect which pixels had their bits flipped. The encrypted images were generated by an exclusive-or operation with pseudo-random bits. The proposed scheme has two distinct versions: a joint method (watermark decoding and image restoration on the decrypted image) and a separate method the encrypted image (generated with) is split by both proposed methods into three distinct sets. Only sets A and B (a total of 2=3 of the image) are used for data hiding, set U is not modified by the embedding algorithm. That can embed data in at most 1=2 of the image (the other half is used for prediction). The data hiding key is used to determine the order in which the pixels in set A and set B are processed. Set A is the first set to be embedded with the hidden data, the pixels in B are considered as possible hosts only after the capacity offered by A is completely exhausted. The pixels in each set are processed as groups of n pixels and a bit of data will be inserted in each group by modifying their t bit value. After decryption, a user with the hiding key can extract the hidden data by determining the order in which the pixels were embedded and reforming the n pixel groups.

Merits: The proposed scheme with no error correction offers a significant increase in capacity

Demerits: The restoring step remains affected by the possibility of errors.

Title: Binary-block embedding for reversible data hiding in encrypted images

Authors: Shuang Yi, Yicong Zhou

Propose a new BBE algorithm for reversible data hiding in the encryption domain, which is totally different from traditional RDH methods. BBE can be utilized in different types of images such as binary, gray-scale, medical and cartoon images. Based on BBE, we further propose a method of reversible data hiding in encrypted images, BBE-RDHEI. Compared with existing state-of-the-art methods, it has significantly improved embedding capacity and quality of the marked decrypted image. BBE-RDHEI can also be simplified and utilized for binary images, while existing RDHEI methods are designed only for gray-scale images. To significantly enhance the security level of BBE-RDHEI, we also propose a security key design mechanism such that BBE-RDHEI is able to resist the differential attack, while existing RDHEI methods cannot. To enhance the robustness of RDHEI methods in withstanding noise and data loss attacks, we introduce a bit-level scrambling

process to BBE-RDHEI after secret data embedding to spread out embedded secret data over the entire marked encrypted image. As a result, BBE-RDHEI is able to recover most of secret data even if one bit-plane (e.g., LSB or MSB) of the marked encrypted image is completely removed. Moreover, any bit-level scrambling algorithm can be used in our BBE-RDHEI. This is another security benefit of BBE-RDHEI.

Merits

A security key design mechanism is proposed to enhance its security level.

Demerits

Image size increases because the used homomorphic encryption algorithm maps the pixel value into a larger data range.

2.5 Title: High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation

Authors: Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng and Xiaojie Guo

Proposed HC_SRDHEI method. For the content owner, the given cover image is represented according to an over-complete dictionary by sparse coefficients. After that, for the given selected patches, the corresponding coefficients and reconstructed residual errors are encoded directly without quantization. For most of the patches, the data size is well reduced in the basis of coefficient representation, thus the vacated room is preserved for high capacity data hiding after image encryption. Note that, for losslessly recovering the cover image, the residual errors are self-embedded into the nonselected patches. The learned dictionary, is also embedded into the encrypted image for further use. At the receiver side, when the receivers accept an encrypted image containing additional data, the processing procedure depends on the role of receiver. If the receiver is a data hider and only has the data hiding key, he can extract the data without knowing the image content. If the receiver is an image owner and only has the encryption key, he can decrypt the image with a better quality. If the receiver is both the image owner and data hider, he has both of two keys in such case. Thus, the data extraction and content recovery are all done, and both results are free of error. In summary, for our proposed framework, the data extraction and image recovery are separable and reversible.

Merits

The proposed method separate the data extraction from image decryption but also achieve excellent performance.

Demerits

Patches contain contextual information and have disadvantages in terms of computation and generalization.

Title: On the Security of Block Scrambling-Based EtC Systems against Extended Jigsaw Puzzle Solver Attacks

Authors: Tatsuya Chuman, Kenta Kurihara, Nonmembers and Hitoshi Kiya

Block scrambling-based image encryption schemes have been proposed for EtC systems, in which a user wants to securely transmit image I to an audience, via a

Social Networking Service (SNS) provider, as illustrated in Fig. 1. Since the user does not give the secret key K to the SNS provider, the privacy of image to be shared is under control of the user even when the SNS provider recompresses image I. Therefore, the user is able to control image privacy for his own demand. On the other hand, in CtE systems, the user has to disclose unencrypted images to recompress them. In the schemes, an image with X × Y pixels is first divided into non-overlapped blocks with Bx × By, then four block scrambling-based processing steps, is applied to the divided

image. Divide an image with X × Y pixels into blocks with Bx × By pixels, and permute randomly the divided blocks using a random integer generated by a secret key K1, where K1 is commonly used for all color components. Using a random integer generated by a key K2, where K2 is commonly used for all color components as well. Apply the negative-positive transformation to each block using a random binary integer generated by a key K3, where K3 is commonly used for all color components. Shuffle three color components in each block (the color component shuffling) using a random senary integer generated by a key K4.

Merits:

Encrypted image has almost the same correlation among pixels in each block as that of the original image, whose property enables to efficiently compress images.

Demerits:

It is confirmed that combining the encryption steps makes puzzle solvers more difficult than single use of each step.

Title: An Encryption-then-Compression System for JPEG/Motion JPEG Standard

Authors: Kenta Kurihara, Masanori Kikuchi, Shoko Imaizumi, Sayaka Shiota, and Hitoshi Kiya

Perceptual image encryption is a processing technique which makes an image difficult to recognize visually. Number theory-based encryption methods, such as RSA, DES or AES are the most secure options. However, in the area of multimedia, many applications have sought a trade-off in security to enable other requirements, including low processing demands, retaining bitstream compliance, and signal processing in the encryption domain, such as compression, watermarking, searching, and so on. In this paper, we focus on image compression systems in the encrypted domain, namely ETC systems, as illustrated in Fig. 1, in which a content owner Alice wants to securely and efficiently transmit an image *I* to a recipient Bob, via an untrusted channel provider Charlie. In particular, the use of the JPEG standard is supposed as a compression method. When a common key is used for all frames, the key management is simple because the number of keys is one totally. However, the difficulty to estimate the key decreases because each frame mutually has some correlation. On the other hand, when an individual key is applied to each frame, the estimation of the keys is more difficult. However, the key management becomes complicated due to a lot of keys. To overcome such situations, we propose a key management scheme the multidimensional hash chain. Figure 8 illustrates the generation and assignment of the encryption keys. The proposed scheme divides a video signal into *N* periods in which each period has *T* frames.

Merits

Provide an efficient ETC system for the JPEG and Motion JPEG standards

Demerits

The key management becomes complicated due to a lot of keys.

Title: Image Manipulation on Social Media for Encryption-then-Compression Systems

Authors: Tatsuya Chuman, Kenta Iida and Hitoshi Kiya

Proposed work focus on two key points regarding image manipulation. The first point is the maximum resolution of uploaded images and the second is the parameters of recompression. Where a user wants to securely transmit image I to an audience, via a SNS provider. Since the user does not give the secret key K to the SNS provider, the privacy of image to be shared is under control of the user, even when the SNS provider decompresses image I. Therefore, the user is able to protect the privacy by him/herself. Even if encrypted images saved in the SNS servers are leaked by malicious users, the third party and general audiences could not see these images visually unless they have key.

Meanwhile, it is known that almost all SNS providers manipulate images uploaded by users, e.g., rescaling image resolution and recompressing with different parameters, for decreasing the data size of ones. Encrypting images might generate images with some distortion due to forcedly image manipulation by SNS providers. Although numerous papers were examined to clarify conditions for resizing image, recompression parameters and conditions have been yet unpublished by SNS providers and researchers. Therefore, we investigate how each SNS provider manipulates images uploaded by users to apply EtC systems to social media.

Merits

Encrypted and non-encrypted JPEG images are uploaded to various SNS providers to confirm the robustness of EtC systems.

Demerits

Sometimes avoid generating block distortion even if the interpolation is carried out.

Title: Bitstream-Based JPEG Image Encryption with File-Size Preserving

Authors: Hiroyuki Kobayashi, Hitoshi Kiya

Proposed a new bitstream-based JPEG image encryption method which allows us to exactly preserve the same file size as the original JPEG bitstream. propose a bitstream-based JPEG encryption scheme that makes the file size exactly equal to the original. Bitstreams encrypted by the proposed method have not only the same file sizes, but also the compatibility with JPEG decoders. Some of only additional bits fields that satisfy conditions are encrypted to keep the compatibility with JPEG decoders. Analysis, byte-by-byte, the entropy-coded data segment and extract additional bits from a byte that satisfies two conditions: the byte includes both Huffman code and additional bits, and the Huffman code includes at least one “0” bit. Generate a random binary sequence with a secret key. Carry out exclusive-or operation between only extracted additional bits and the random sequence and replace the additional bits with the result. Produce an encrypted bitstream by combining the encrypted additional bits with other data without any encryption. The data consist of a 5-bit Huffman code and 3-bit additional bits. Even if all the additional bits are 1, the entire byte never becomes “FF”. Therefore, the additional bits part is able to be encrypted. The second byte: The data consist of 3-bit additional bits and a 5-bit Huffman code. In the original data, since the additional bit was “111” and the remaining Huffman code was ‘111111”, “FF” was composed as the whole byte. If any bit of the additional bit is changed to 0 by encryption, the entire byte is not ‘FF’ and ‘00’ of the third byte is not inserted. Since this causes a file size change, the additional bits of the second byte are not encrypted. The data are padding data because the second byte is “FF”. Since this is not an additional bit, it is not encrypted. The data consist of a 1-bit Huffman code and 7-bit additional bits. Even if all the additional bits are 1, the entire byte never becomes “FF”. Therefore, the additional bits part is able to be encrypted.

Merits:

It allows us to preserve the same file size before and after the encryption.

Demerits:

Does not consider image transmissions are successfully carried out after the hooking encryption process.

Title: Separable Reversible Data Hiding in Encrypted JPEG Bitstreams

Author: Zhenxing Qian, Hang Zhou, Xinpeng Zhang and Weiming Zhang

Proposed work focuses on RDH in encrypted JPEG bitstream, the most popular image format, aiming at providing an RDH-EI approach with separable extraction capability, high embedding capacity, and secure encryption. We first propose an encryption scheme for enciphering JPEG

bitstreams. Based on JPEG encryption, a reversible data hiding method is developed for service providers to embed additional bits. Finally, we propose an iterative algorithm to recover the original image. In this work, lossless recovery is required. Although JPEG encoding itself is lossy, users always hope not to introduce further degradation to a JPEG image while uploading. That is why lossless recovery is required. The JPEG RDH-EI workflow includes three parties: content owner, data hider, and recipient. Given a JPEG bitstream and an encryption key, the content owner generates a ciphertext bitstream after syntax parsing and encryption. In the process, the file size is kept unchanged and the format is compliant to common JPEG decoders. When a remote server receives the encrypted bitstream, the data hider parses the bitstream and hides additional messages in it using an embedding key. After the marked encrypted bitstream is constructed, the file size and format compliance are preserved. In this scheme, the server can extract additional messages from the marked encrypted bitstream using the embedding key. On the recipient side, the additional messages can also be extracted from the received bitstream if the embedding key is available. A recipient with only the encryption key can view an approximate image by a direct decryption. If both the encryption and embedding keys are available, the recipient can losslessly recover the original bitstream after decrypting the marked encrypted JPEG bitstream.

Merits:

Database administrator cannot read the hidden messages from the marked encrypted bitstream.

Demerits:

It is difficult to design a secure encryption algorithm for JPEG.

III. RESEARCH METHODOLOGY

3.1 EXISTING APPROACH

RHD-EI allows a server to embed additional message into an encrypted image uploaded by the content owner, and guarantees that the original content can be losslessly recovered after decryption on the recipient side. Generally, reversibility is closely related to the embedding payload. If the original image can be losslessly recovered when the payload does not exceed the achievable capacity, say it is reversible.

This method strictly relies on the properties of secret sharing. Summarizing the main techniques, secret sharing serves as the underlying primitive offering security, multiple secret preserves size complexity, and inherently additive homomorphism realizes the data embedding. Here provide the formal description of the technique, and present a clear notion, so-called operating addition homomorphism in multi-secret sharing (OAMSS). Also provide another technique to compress the size of a key used in OAMSS. For generalization, if SNK (Share No Secret Key) schemes satisfy some properties, they can be converted to SOK (Share One Key). Hence, this method can be generalized as a converter. As a concrete instantiation, SNK scheme based on difference expansion, we show the SOK-type RDHEI by slight modification. The scheme overview is described as follows. P will pre-process the cover-image and generate a new cover-image, referred to as the processed image, and then send H the encrypted image by using polynomial interpolation. H will obtain a new polynomial which carries a secret message in the released LSB plane, and then use addition homomorphism to generate the encrypted image with embedded message. Finally, by decryption R is able to obtain the stego-image, and then recover the cover-image and secret message.

Disadvantages

- It applicable only for JPEG images.
- Creating meaningless shares initiates the intruder to try and decrypt the shares.

3.2 PROPOSED APPROACH

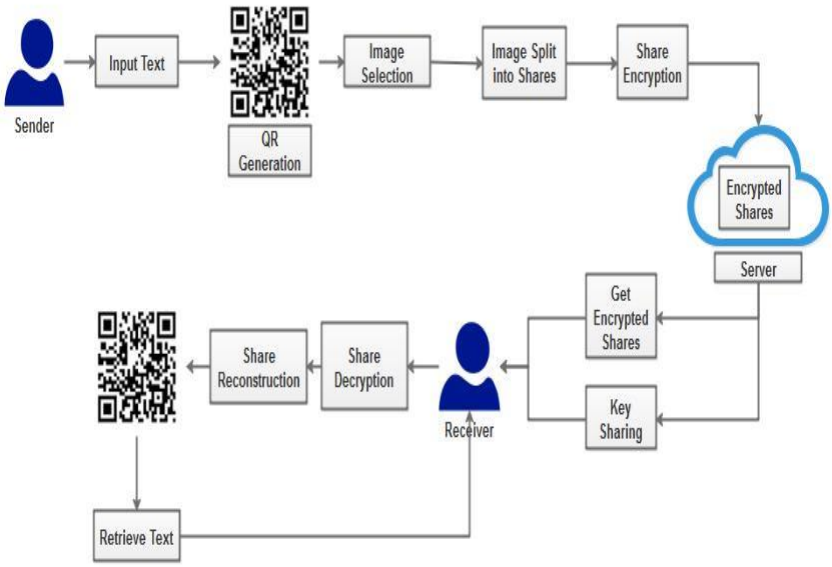
The main objective of this project is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. This method eliminates the fundamental security challenges of VC like external use of code book, random share patterns, expansion of pixels in shared and recovered images, lossy recovery of secret images and limitation on number of shares. The proposed method is n out of n multi secret sharing scheme. Transmission of multiple secret images simultaneously is achieved through this proposed work. The secret text can be hidden within the image in QR format. Teat message was created by sender and converted into QR code format. The secret image can be revealed only when all the n shares are received by the receiver and decrypted. The text is typed and hidden in an image. This is done using LSB method. Then the XOR based VC method is used to encrypt the image and send it to the receiver. The key which is used to encrypt the shares will be mailed to the receiver. The receiver will decrypt the shares using the same key that is used for encryption. After that, the hidden text will be extracted from the recovered image using the LSB method.

Advantages

- The secret image and the recovered image will be of the same size.
- Multi secret sharing is used to send multiple shares at the same time.
- The hidden text is very safe.

PROPOSED ARCHITECTURE

Software architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes. A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability. Software architecture must describe its group of components, their connections, interactions among them and deployment configuration of all components.



IV. FOOTNOTES

The proposed method describes how a secret image is securely communicated from source to destination. In this work, a text message was hidden within QR Code then the QR will be hidden within image. The sender has to create text and generate QR for input text then select the image to hide the QR image using MPVD with LSB approach that should be sent the message secretly to the receiver. Then the secret image is splitted into "n" number of shares. Each share is encrypted using XOR operation. Then, all the encrypted shares are transmitted in a single transmission to the receiver. The receiver should use the decryption key to decrypt the shares. After decrypting, the individual shares will be joined together to form the recovered (original) image. The recovered image will be of the same size as the original image.

REFERENCES

Future Work

Steganography will continue to increase in popularity over cryptography. It is well accepted though, small sentences and one-word answers example a "yes" are virtually impossible to find. This could be an area for further advances as possible compression sizes decreases further. There also seems very little in terms of tools for hiding data in videos. There are some for audio, but this is still an area, which lags behind image steganography. The future may see audio files and video streams that could possibly be decoded on the fly to form their correct messages.

REFERENCES

1. Zhou, Jiantao, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang. "Secure reversible image data hiding over encrypted domain via key modulation." IEEE transactions on circuits and systems for video technology 26, no. 3 (2015): 441-452.
2. Bartwal, Monika, and Rajendra Bharti. "Lossless and Reversible Data Hiding in Encrypted Images With Public Key Cryptography." Annals of Computer Science and Information Systems 10 (2017): 127-134.
3. Dragoi, Ioan Catalin, Henri-George Coanda, and Dinu Coltuc. "Improved reversible data hiding in encrypted images based on reserving room after encryption and pixel prediction." In 2017 25th European Signal Processing Conference (EUSIPCO), pp. 2186-2190. IEEE, 2017.
4. Yi, Shuang, and Yicong Zhou. "Binary-block embedding for reversible data hiding in encrypted images." Signal Processing 133 (2017): 40-51
5. Cao, Xiaochun, Ling Du, Xingxing Wei, Dan Meng, and Xiaojie Guo. "High capacity reversible data hiding in encrypted images by patch-level sparse representation." IEEE transactions on cybernetics 46, no. 5 (2015): 1132-1143.
6. Chuman, Tatsuya, Kenta Kurihara, and Hitoshi Kiya. "On the security of block scrambling-based etc systems against extended jigsaw puzzle solver attacks." IEICE TRANSACTIONS on Information and Systems 101, no. 1 (2018): 37-44.

7. Kurihara, Kenta, Masanori Kikuchi, Shoko Imaizumi, Sayaka Shiota, and Hitoshi Kiya. "An encryption-then-compression system for jpeg/motion jpeg standard." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 98, no. 11 (2015): 2238-2245.
8. Chuman, Tatsuya, Kenta Iida, and Hitoshi Kiya. "Image manipulation on social media for encryption-then-compression systems." In 2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), pp. 858-863. IEEE, 2017.
9. Kobayashi, Hiroyuki, and Hitoshi Kiya. "Bitstream-Based JPEG Image Encryption with File-Size Preserving." In 2018 IEEE 7th Global Conference on Consumer Electronics (GCCE), pp. 384-387. IEEE, 2018.
10. Qian, Zhenxing, Hang Zhou, Xinpeng Zhang, and Weiming Zhang. "Separable reversible data hiding in encrypted JPEG bitstreams." IEEE Transactions on Dependable and Secure Computing 15, no. 6 (2016): 1055-1067.
11. Radha Krishnan, B., Vijayan, V., Parameshwaran Pillai, T. and Sathish, T., 2019. Influence of surface roughness in turning process—an analysis using artificial neural network. Transactions of the Canadian Society for Mechanical Engineering, 43(4), pp.509-514.
12. Krishnan, B.R., Ramesh, M., Giridharan, R., Sanjeevi, R. and Srinivasan, D., Design and Analysis of Modified Idler in Drag Chain Conveyor. International Journal of Mechanical Engineering and Technology, 9(1), pp.378-387.
13. Krishnan, B.R., Vijayan, V. and Senthilkumar, G., 2018. Performance analysis of surface roughness modelling using soft computing approaches. Applied Mathematics & Information Sciences, 12(6), pp.1209-1217.
14. KRISHNAN, B.R. and PRASATH, K.A., 2013. Six Sigma concept and DMAIC implementation. International Journal of Business, Management & Research (IJBMR), 3(2), pp.111-114.

