ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 111-116 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp20.pdf

Novel Approach for Image Encryption then Compression System based on the Prediction error clustering and random permutation

Mr. Sk.Manjoor[1], Dr. P. Harini[2]

[1]*II M.Tech. - II Sem., Dept. of CSE, St. Ann's College of Engineering. & Technology. Chirala, Andhra Pradesh -,523 187 INDIA,*
shaik.mannu@gmail.com
[2]*Professor &Head , Dept. of CSE, St. Ann's College of Engg. & Tech., Chirala, A. P, INDIA*
drharinicse@gmail.com

ABSTRACT:-In numerous down to earth situations, picture encryption must be directed before picture pressure. This has prompted the issue of how to outline a couple of picture encryption and pressure calculations such that packing the scrambled pictures can in any case be proficiently performed. In this paper, we outline a profoundly effective picture encryption-then-pressure (ETC) framework, where both lossless and misfortune pressure is considered. The proposed picture encryption plan worked in the forecast blunder area is indicated to have the capacity to give a sensibly abnormal state of security. We additionally exhibit that a number juggling coding-based methodology can be abused to proficiently pack the scrambled pictures. All the more outstandingly, the proposed pressure approach connected to encoded pictures is just somewhat more awful, as far as pressure proficiency, than the cutting edge lossless/misfortune picture coders, which take unique, decoded pictures as inputs. Conversely, a large portion of the current ETC arrangements incite huge punishment on the pressure effectiveness.

INTRODUCTION:-

CONSIDER an application situation in which a substance proprietor Alice needs to safely and efficiently transmit a picture I to a beneficiary Bob, by means of an untrusted channel supplier Charlie. Ordinarily, this should be possible as takes after. Alice first packs I into B, and after that encodes B into I.e. utilizing an encryption capacity EK (•), where indicates the mystery key, as showed in Fig. 1(a). The scrambled information I.e. is then gone to Charlie, who just advances it to Bob. After accepting I.e., Bob successively performs unscrambling and decompression to get a reproduced picture ˆ I. Despite the fact that the above Compression-then-Encryption (CTE) worldview meets the prerequisites in numerous protected transmission situations, the request of applying the pressure and encryption should be turned around in some different circumstances. As the substance proprietor, Alice is constantly intrigued by ensuring the security of the picture information through encryption. By and by, Alice has no motivation to pack her information, and thus, won't utilize her restricted computational assets to run a pressure calculation before scrambling the information. This is particularly genuine when Alice utilizes an asset denied cell phone. Interestingly, the channel supplier Charlie has an overriding enthusiasm for compacting all the system traffic to expand the system usage. It is in this way greatly craved if the pressure undertaking can be assigned by Charlie, who commonly has bottomless computational assets. A major test inside such

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 111-116 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp20.pdf

Encryption-then-Compression (ETC) structure is that pressure must be led in the encoded space, as Charlie does not access to the mystery key K. This sort of ETC framework is exhibited in Fig. 1(b).

The likelihood of handling encoded flags specifically in the scrambled space has been getting expanding consideration as of late [2]–[6]. At the first look, it is by all accounts infeasible for Charlie to pack the scrambled information, since no sign structure can be misused to empower a customary compressor. Albeit nonsensical, Johnson et. al demonstrated that the stream figure scrambled information is compressible through the utilization of coding with side data standards, without bargaining either the pressure efficiency or the data theoretic security [7]. Notwithstanding the hypothetical findings, [7] additionally proposed down to earth calculations to drowsily pack the encoded paired pictures. Schonberg et. al later researched the issue of packing encoded pictures when the hidden source insights is obscure and the sources have memory [8], [9]. By applying LDPC codes in different bit-planes and misusing the bury/intra relationship, Lazzeretti and Barni introduced a few techniques for misfortune less pressure of encoded grayscale/shading pictures [11]. Moreover, Kumar and Makur connected the methodology of [7] to the forecast blunder area and accomplished better lossless pressure execution on the scrambled grackle/shading pictures [12]. Helped by rate-good punctured turbo codes, Liu et. al added to a dynamic technique to lossless com-press stream figure encoded grayscale/shading pictures [13]. All the more as of late, Klink et al. extended Johnson's structure to the instance of packing square figure scrambled To achieve higher compression ratios, lossy pressure of scrambled information was likewise mulled over [14]. Zhang et.al proposed a versatile misfortune coding system of encoded pictures by means of a multi-determination development [14]. In [13], a compressive detecting (CS) instrument was used to pack scrambled pictures came about because of direct encryption. A modified premise interest calculation can then be connected to gauge the first picture from the compacted and scrambled information. Another CS-based methodology for scrambling packed pictures was accounted for in Furthermore, Zhang composed a picture encryption plan by means of pixel-space stage, and showed that the encoded file can be efficiently compacted by disposing of the unreasonably unpleasant and fine data of coefficients in the change area [10]. As of late, Zhang et. al recommended another pressure approach for scrambled pictures through multi-layer decay [11]. Expansions to visually impaired pressure of scrambled features were produced in [11], [12]. Regardless of broad endeavors as of late, the current ETC frameworks still miss the mark in the pressure execution, contrasted and the best in class lossless/lossy picture and feature coders that oblige decoded inputs. The essential center of this work is on the down to earth outline of a couple of picture encryption and pressure plans; in a manner that com-squeezing the encoded pictures is similarly efficient as compacting their unique, decoded partners. In the mean time, sensibly abnormal state of security should be guaranteed. If not generally specified, 8-bit grayscale pictures are accepted. Both lossless and lossy pressure of scrambled pictures will be considered. Specifically, we propose a stage based picture encryption methodology led over the forecast slip space. A connection versatile math coding (AC) is then indicated to have the capacity to efficiently pack the encoded information. On account of the about i.e. property of the expectation mistake

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 111-116 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp20.pdf

succession, immaterial pressure punishment (< 0.1% coding misfortune for lossless case) will be presented. Moreover, because of the high affectability of expectation lapse arrangement against aggravations, sensibly abnormal state of security could be held. Whatever is left of this paper is composed as takes after. Segment II gives the subtle elements of our proposed ETC framework, where lossless pressure is considered. Expansion to the instance of lossy pressure is given in Section III. In Section IV, we display the security investigation and assessment of the pressure execution. Test results are accounted for in Section V to accept our findings. We conclude in Section VI.

RELATED WORK:-

In this section, the security of our proposed image encryption and the compression performance on the encrypted data are evaluated experimentally. Fig. 6 illustrates the Lena and Baboon images, together with their encrypted versions, from which we can see that our encryption approach is effective in destroying the semantic meaning of the images. In addition, it can be observed that the encrypted Baboon image looks 'brighter' than the encrypted Lena image. This is because the Baboon image contains large portion of texture regions that are

Difficult to compress, resulting in more large-valued prediction errors. We implement the attack strategy of directly decoding the encrypted file I.e., as described in Section IV-A. Ten images of size 512 × 512 shown in Fig. 7 are used as the test set. In Fig. 8, we give the PSNR results of the reconstructed images, where x-axis represents the image ID. It can be observed that all the PSNR values are around 10 dB, which is too low to convey any useful semantic information.

We also evaluate the reconstruction performance under the assumption that the bounded errors only occur in the prediction errors of the first two rows, while all the remaining ones are perfectly known. Here the estimation error bound ε is set to be 5. Fig. 9 illustrates the PSNR values of the reconstructed images, where each point is the averaged result of 10 realizations. It can be seen that, even under such favourable conditions, the attacker still cannot obtain any useful visual information of the source images, because all the PSNR values are too low (around 10 dB). In Table I, the compression efficiency of our proposed method applied to the encrypted images is compared with the lossless rates given by the latest version of CALIC, a benchmark of practically good lossless image codecs, and the method in [13], a state-of-the-art lossless compression approach on encrypted images. The test set is composed of 100 images with various characteristics, 10 of which are shown in Fig. 7. Here 'B' and 'bpp' denote bytes and bit per pixel, respectively. In the rightmost two columns, Sc and S[13] stand for the bit rate saving of our proposed method over the CALIC and the method in [13], respectively. All the results of the proposed method are obtained by averaging over 10 random trials. The last row gives the averaged results over the 100 images in the test set. It can be seen that the coding penalty incurred by our method is consistently lower than 0.1% when comparing with the results of the CALIC. Meanwhile, the bit rate sparing over the strategy in [13] can be up to 36.3%, which is accomplished by the picture Airplane.

In this segment, we show the points of interest of the three key segments in our proposed ETC framework, in particular, picture encryption led

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 111-116 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp20.pdf

by Alice, picture pressure led by Charlie, and the successive unscrambling and decompression directed by Bob.

A. Image Encryption via Prediction Error Clustering and Random Permutation: - From the perspective of the whole ETC system, the design of the encryption algorithm should simultaneously consider the security and the ease of compressing the encrypted data. To this end, we propose an image encryption scheme operated over the prediction error domain. The schematic diagram of this image encryption method is depicted in Fig. 2. For each pixel $I_{i,j}$ of the image I to be encrypted, a prediction $\bar{I}_{i,j}$ is first made by using an image predictor, e.g. GAP [21] or MED [22], according to its causal surroundings. In our work, the GAP is adopted due to its excellent de-correlation capability. The prediction result $\bar{I}_{i,j}$ can be further refined to $\tilde{I}_{i,j}$ through a context-adaptive, feedback mechanism [21]. Consequently, the prediction error associated with $I_{i,j}$ can be computed by

$$E_{i,j} = I_{i,j} - \tilde{I}_{i,j} \quad (1)$$

Although for 8-bit images, the prediction error ei,j can potentially take any values in the range [−255,255], it can be mapped into the range[0,255], by considering the fact that the predicted value ˜ Ii,j is available at the decoder side. From (1), we know that ei,j must fall into the interval[−˜ $I_{i,j}$,255−˜ Ii,j], which only contains 256 distinct values. More specifically, if ˜ $I_{i,j} \leq 128$, we rearrange the possible prediction errors−˜$I_{i,j}$−˜ $I_{i,j}$ +1,...,0,1,...,˜ $I_{i,j}$, ˜ $I_{i,j}$ +1,...,255− ˜ Ii,jin the order 0,+1,−1,...,+˜ $I_{i,j}$,−˜ $I_{i,j}$, ˜ $I_{i,j}$ + 1, ˜ $I_{i,j}$ + 2,..., 255− ˜ $I_{i,j}$, each of which is sequentially mapped to a value between 0 to 255. If ˜ $I_{i,j} > 128$, a similar mapping could be applied. Note that, in order to reverse the above mapping, the predicted value ˜ $I_{i,j}$ needs to be known. In the sequel, let us denote the mapped prediction error by ˜ ei,j, which takes values in the range [0,255].

Our proposed image encryption algorithm is performed over the domain of the mapped prediction error ˜ ei,j. Instead of treating all the prediction errors as a whole, we divide the prediction errors into L clusters based on a context-adaptive approach. The subsequent randomization and compression will be shown to be benefited from this clustering operation. To this end, an error energy estimator originally proposed in [21] is used as an indicator of the image local activities. More specifically, for each pixel location (i, j), the error energy estimator is defined by

$$\Delta_{i,j} = dh + dv + 2|e_{i-1,j}| \quad (2)$$

Where

$$dh = |I_{i-1,j} - I_{i-2,j}| + |I_{i,j-1} - I_{i-1,j-1}| + |I_{i,j-1} - I_{i+1,j-1}|$$

$$dv = |I_{i-1,j} - I_{i-1,j-1}| + |I_{i,j-1} - I_{i,j-2}| + |I_{i+1,j-1} - I_{i+1,j-2}| \quad (3)$$

And $e_{i-1,j}$ is the prediction error at location (i − 1, j). The configuration of the group ought to at the same time consider the security and the simplicity of compacting the scrambled information. In a logged off preparing procedure, we gather an arrangement of tests (˜ e,) from suitable preparing pictures. A dynamic programming method can then be utilized to get an ideal bunch in least entropy sense, i.e., pick 0= q0 < q1 < •••<qL =∞such that the accompanying contingent entropy measure is

$$\sum_{0 \leq i \leq L-1} H(\tilde{e}|q_i \leq \Delta < q_{i+1}) p(q_i \leq \Delta < q_{i+1}) \quad (4)$$

WhereH(·) is the 1-D entropy function taking logarithm in base 2. It can be seen that the term H(˜ e|qi ≤ <qi+1) denotes the entropy of the prediction error sequence in the ith cluster, and hence, (4) becomes an approximation of thebit rate

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 111-116 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp20.pdf

(in bpp) of representing all the prediction errors. Therefore, the cluster designed by minimizing (4) is expected to achieve optimal compression performance. Also, the selection of the parameter L needs to balance the security and the encryption complexity. Generally, larger L could potentially provide higher level of security because there are more possibilities for the attacker to figure out. However, it also incurs higher complexity of encryption. We heuristically find that L = 16 is an appropriate choice balancing the above two factors well. Note that the cluster configurations, i.e. the values of all qi, are publicly accessible. For each pixel location (i, j), the corresponding cluster index k can be determined by

$$k = \{k|q_k \leq \Delta_{i,j} < q_{k+1}\} \quad (5)$$

b)Lossless Compression of Encrypted Image Via Adaptive AC:- The compression of the encrypted file Ie needs to be performed in the encrypted domain, as Charlie does not have access to the secret key K. In Fig. 4, we show the diagram of lossless compression of Ie. Assisted by the side information |˜ Ck|, for $0 \leq k \leq L-2$, a de-assembler can be utilized to parse Ie into L segments ˜ C0, ˜ C1,...,˜ CL−1 in the exactly same way as that done at the encryption stage. An adaptive AC is then employed to lossless encode each prediction error sequence ˜ Ck into a binary bit stream Bk. Note that the generation of all Bk can be carried out in a parallel manner to improve the throughput. Eventually, an assembler concatenates all Bkto produce the final compressed and encrypted bit stream B, namely,

$$B = B0B1 \ldots BL-1 \quad (7)$$

C. Sequential Decryption and Decompression: - Upon receiving the compressed and encrypted bit stream B, Bob aims to recover the original image I. The schematic diagram demonstrating the procedure of sequential decryption and decompression is provided in Fig. 5. According to the side information |Bk|, Bob divides B into L segments Bk,for $0 \leq k \leq L - 1$, each of which is associated with a cluster of prediction errors. For each Bk, an adaptive arithmetic decoding can be applied to obtain the corresponding permuted prediction error sequence ˜ Ck. As Bob knows the secret key K, the corresponding de-permutation operation can be employed to get back the original Ck.

$$I_{i,j} = \tilde{} I_{i,j} + e_{i,j} \quad (9)$$

As the predicted value ˜ Ii,j and the error energy estimator i,j are both based on the causal surroundings, the decoder can get the exactly same prediction ˜ Ii,j. In addition, in the case of lossless compression, no distortion occurs on the prediction error ei,j, which implies $\hat{} I_{i,j} = I_{i,j}$, i.e., error-free decoding is achieved.

CONCLUSION:-

In this paper, we have designed an efficient image Encryption-then-Compression (ETC) system. Within the pro- posed framework, the image encryption has been achieved via prediction error clustering and random permutation. Highly efficient compression of the encrypted data has then been realized by a context-adaptive arithmetic coding approach. Both theoretical and experimental results have shown that reasonably high level of security has been retained. More notably, the coding efficiency of our proposed compression method on encrypted images is very close to that of the state- of-the-art lossless/lossy image codecs, which receive original, unencrypted images as inputs.

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 111-116 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp20.pdf

REFERENCES:-

[1] J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryption- then-compression system," in Proc. ICASSP, 2013, pp. 2872–2876.
[2] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.
[3] T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357.
[4] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.
[5] M. Barni, P. Failla, R. Lazzeretti, A.-R.Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 452–468, Jun. 2011.
[6] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating pri- vate recommendations efficiently using homomorphic encryption and data packing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1053–1066, Jun. 2012.
[7] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
[8] D. Schonberg, S. C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in Proc. 43rd Annu. Allerton Conf., 2005, pp. 1–3.
[9] D. Schonberg, S. C. Draper, and K. Ramchandran, "On compression of encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 269–272.
[10] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers," IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.
[11] R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and colour images," in Proc. 16th Eur. Signal Process. Conf., Aug. 2008, pp. 1–5.
[12] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in Proc. MMSP, 2008, pp. 760–764.
[13] W. Liu, W. J. Zeng, L. Dong, and Q. M. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image.Process, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[14] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," IEEE Trans. Imag. Process, vol. 21, no. 6, pp. 3108–3114, Jun. 2012.

AUTHORS:

Mr. Sk.Manjoor Studying II M.Tech (CSE) in St. Ann's College of Engineering & Technology, Chirala, He completed B.Tech.(IT) in 2012 in St. Ann's Engineering College, Chirala.

Dr. P.Harini is presently working as Professor & Head, Department of Computer science &Engineering in St. Ann's College of Engineering and Technology, Chirala. She Completed Ph.D. in Distributed and Mobile Computing from JNTUA. She guided many U.G. & P.G projects. She has more than 19 Years of Teaching and 2 Years of Industry Experience. She published more than 20 International Journals and 25 research Oriented Papers in various areas. She was awarded Certificate of Merit by JNTUK., Kakinada on the University Formation day, 21st August 2012.