Secure Image Transformation Using Remote Sensing Encryption Algorithm

Mr.Rafeeque KM, Mr.S.Siva Shankar
Department of Computer Science and Engineering
Nehru College of Engineering and Research Center, Pampady, Thrissur, Kerala.
rafeequekm50@gmail.com,sss_siva85@yahoo.co.in

Abstract: In today's heterogeneous network environment, there is encryption is used to securely transmit data in open networks. In this paper, we introduce an encoded transformation based on the combination of image transformation and a well known encryption. Each type of data has its own features; therefore different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. In this paper, we propose a new kind of security model. Under the proposed model efficient protocols on two basic image processing algorithms – linear filtering and thresholding – are developed. For both problems we consider two situations: 1) only two parties are involved where one holds the data and the other possesses the processing algorithm; 2) an additional non-colluding third party exists. Experiments show that our proposed protocols improved the computational time and secure images. There is a growing de-mand for distrusted parties to jointly execute remote sensing algorithms on private data whose secrecy needed to be safeguarded. Platforms that support such computation on image processing purposes are called secure image processing protocols. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the remote sensing algorithm. The results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

Keywords: Image transformation, Image decoding, Image encryption, Security Analysis.

I. Introduction

The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet [1]. Data encryption is widely used to ensure security however, most of the available encryption algorithms are used for text data. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data [2]-[4]. In general, transforming images from a source space to a target space is difficult. Natural images are very high dimensional, statistically non-Gaussian and exhibit abundant varying texture patterns. Directly learning image models and their mapping relations may not be feasible. Even working on local patches, the dimensionality is still too high to learn a good and explicit mapping function. The above reviewed methods either use nonparametric approaches, such as nearest neighbour (NN) searching, and learn the mapping relations using the found neighbour training patch pairs [4], [7], or use nonlinear regression based on summarizing the training data using a small number of prototype patches [11], [12]. When dealing with a huge amount of training patches, searching NNs could be prohibitively slow and also costs large memory. Although there exist acceleration methods such as approximate nearest neighbour (ANN) search [16], [15], they cannot generally cope with the memory cost problem. For nonlinear regression [11], [12], when the prototype number is getting large, significant computation is required, while fewer prototypes cannot approximate the image space well. The proliferation of imaging and storage devices and the ubiquitous presence of computer networks make sharing of digital data easier than ever. Such casual exchange of data, however, has increasingly raised questions on how sensitive information can be protected. Consider the scenario in which a user of a cellular-phone camera wants to send his pictures to an online photo-processing laboratory for image enhancement such as red-eye removal. The user would be concerned about the privacy of his pictures while the online store would need to protect the proprietary enhancement technologies against reverse-engineering. One way of solving this problem is the Trusted Computing (TC) Platform where the software is executed in a secure memory space of the client machine equipped with a cryptographic co-processor [17]. Besides the high cost of overhauling the existing PC platform, the TC concept remains highly controversial due to its unbalanced protection of the software companies over the consumers [3]. To balance the pre- tection for both the clients and the servers, another solution is then proposed by establishing a joint computation and communication plat- form that can guarantee the secrecy of private data and algorithms and at the same time achieve a well-defined objective that benefits all parties involved. Platforms that provide security to the joint image processing algorithms are called secure image processing protocols.

II. Related Work

Encryption is the process of transforming the information to insure its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. As a result, different security techniques have been used to provide the required protection [8]. The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images [9].

Image encryption techniques try to convert an image to another one that is hard to understand [9]. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. Our method also falls in a broader category of remote sensing encryption (RSE). A popular choice of RS is based on Gaussian Mixture Models (GMM) [6], which describes local image patches with a mixture of Gaussian distributions. The GMM model learning is to divide the data (image patches) into precise and representative local clusters. This might be applicable to image restoration problems where it could be case that only patches of the observed (degraded) image itself are involved in clustering. This is exactly the approach taken in [7], where the Remote Sensing Encryption algorithm was used for the clustering purpose. The general image mapping problems using a large training set of paired images, it is very difficult to achieve precise clustering, which requires a huge number of local neighbourhoods. Similar to k-means clustering, in such a scenario the RSE algorithm considered in [7] could be prohibitively slow. For these methods, it also requires high computational complexity to retrieve local clusters (Gaussians) in the estimation process.

One of the well-established image transformation approaches is Freeman et al.'s NN example-based learning Huffman coding [4]. Given a test image in the source space, each patch of the test image is compared with the training patches in the source image space, and its several nearest neighbours are selected as candidates. To reconstruct the target image, the candidate patches in the target space are selected and stitched using Markov random fields (MRF). The same approach is also applied to face sketch synthesis [5]. Since this method uses only one of the nearest neighbours for reconstruction, it is susceptible to suffering from over fitting, visually producing noisy and/or jaggy artifacts. As extensions, neighbour embedding [7] made benefits of multiple NNs, and mixture of mapping experts [11] was learned by locally linear regression. The transformation technique works as follows: the *original* image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the encryption algorithm. The main idea is that an image can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. [5]

In terms of performing mappings in projected feature spaces, Lin and Tang [10] found the most correlative subspaces of different image styles, and performed regression at the reduced subspace dimensions. For each style, it could find only one common subspace, limiting its applicability to only mapping of face images with regular structure. Li and Adelson [9] computed image wavelet coefficients and considered "nested binning" sub band coefficients of local neighbourhood centred at each training image pixel. However, nested binning simplified high dimensional space partitioning as independent partitioning along each feature dimension (sub band), and thus produced lots of empty hyper-rectangular bins. Mairal et al. [3] also considered dictionary learning for image transformation. They proposed a supervised learning method to learn a dictionary in the source image space and a corresponding transformation matrix. The learned global transformation matrix was used to map sparse features of source image patches to intensity values of target patches. Instead, our method is based on a local regression approach that learns transformation parameters for each of a great number of local clusters. Consequently, our method admits a much richer model, resulting in improved mapping power than the global method used in [6]. Although supervised learning may result in a dictionary better adapted to the task at hand, the global transformation model used limits its applicability to only image restoration applications, e.g., a classical inverse half toning problem, as considered in [6]. It is unclear how their method can perform on more general image transformation applications.

III. Image encryption

Encryption is the process of transforming the information to insure its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. As a result, different security techniques have been used to provide the required protection [8]. The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today.

Measurement		A	B	C	D
Correlation	Horizontal	0.933	0.035	0.843	0.034
	Vertical	0.936	0.107	0.844	0.038
	Diagonal	0.919	0.032	0.748	0.013
	Opposite Diagonal	0.916	0.034	0.745	0.009
	Average	0.926	0.052	0.795	0.023
Entropy value		2.431	4.799	2.431	5.231

Table 1: Results of encryption

Besides data structures, search quality and efficiency critically depend on the concise feature representation of signals and the proximity measure. Our image transformation is based on the learned sparse feature representation. While the sparse representation of patch

samples is in high dimensions, those nonzero features are very sparse and essentially correspond to salient patch structures identified by corresponding dictionary atoms. When devising a data structure for efficient retrieval of the closest cluster for a query patch, it is beneficial to take advantage of such a high dimensional but sparse feature representation of signals. Besides sparsity, we have additional information of the dimension selection order in sparse coding of image patches via solving (4) and (6). While most of the existing methods use Euclidean distance for similarity search, we argue that the dimension selection order in sparse vector representation.

Also provides important criteria for matching similar patches.. A load balancing algorithm which is dynamic in nature does not consider the previous state or behavior of the system, that is, it depends on the present behavior of the system. The important things to consider while developing such algorithm are : estimation of load, comparison of load, stability of different system, performance of

system, interaction between the nodes, nature of work to be transferred, selecting of nodes and many other ones.

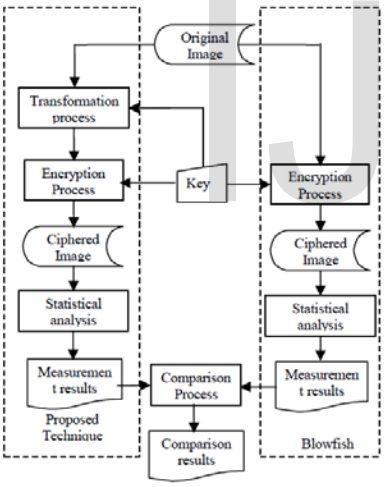

Fig 1: The diagram of the proposed method

The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image. The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbours. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbours. At the receiver side, the original image can be obtained by the inverse transformation of the blocks. Our method falls in the first category.

Training paired patches are extracted from observed gray scale images and their shading components, where the mean (DC) of each patch is removed. Intrinsic image estimation is realized by estimating sparse feature vector at each pixel of the target image. To reconstruct the target image, we use MRF optimization: Since dictionary atoms are DC-free, for the estimated patches cantered at each pixel we compute their optimal mean values by iterative conditional mode [5]. Final reconstruction of the target image is obtained by averaging DC returned estimated patches at overlapped pixels**.** Consistent with qualitative comparison, our method gives smaller quantitative error than other single gray scale image-based methods, and as small as that using additional color information.

Measurement	Number of blocks	A	B	C	D
Average correlation	30 × 30	0.9257	0.0519	0.7952	0.0234
	60 × 60			0.6681	0.0092
	100 ×100			0.5211	0.0056
Entropy	30 × 30	2.4305	4.799	2.4305	5.2305
	60 × 60				5.4737
	100 ×100				5.5281

Table 2: Results of correlation

The correlation and entropy of the three images are computed and compared with each other. This technique aims at enhancing the security level of the encrypted images by reducing the correlation among image elements and increasing its entropy value.

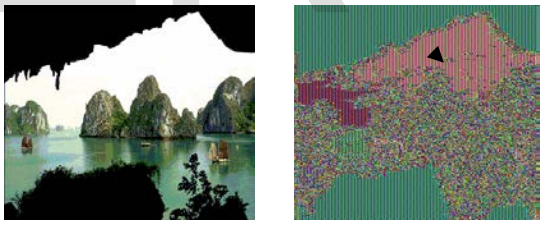

Fig 2: Image decomposition

The result of neighbour embedding is not as sharp as ours. The soft edge prior can produce color attractive results, but also introduce some smoothing effect that is sometimes undesired. Compared with [13], our results look more photorealistic. To quantitatively compare different methods, we report in Table 5 the RMS errors for the images in Fig. 2, available in the online supplemental material. Consistent with the visual comparison, our method gives the lowest reconstruction errors using the original HR image as ground truth. Different choices of t may have effects on our results. The available in the online supplemental material, for a discussion of sparsity level effect.

IV. Image Decoding

This mathematical operation converts each frame/field of the video source from the spatial (2D) domain into the frequency domain (aka transform domain.) A perceptual model based loosely on the human psycho visual system discards high-frequency information, i.e. sharp transitions in intensity, and color hue. In the transform domain, the process of reducing information is called quantization. In simpler terms, quantization is a method for optimally reducing a large number scale (with different occurrences of each number) into a smaller one, and the transform-domain is a convenient representation of the image because the high-frequency coefficients, which contribute less to the over picture than other coefficients, are characteristically small-values with high compressibility. The quantized coefficients are then sequenced and losslessly packed into the output bit stream. Nearly all software implementations of JPEG permit user control over the compression-ratio (as well as other optional parameters), allowing the user to trade off picture-quality for smaller file size. In embedded applications (such as miniDV, which uses a similar DCT-compression scheme), the parameters are pre-selected and fixed for the application. Before computing the DCT of the 8×8 block, its values are shifted from a positive range to one centered around zero. For an 8-bit image, each entry in the original block falls in the range $[0, 255]$. The midpoint of the range (in this case, the value 128) is subtracted from each entry to produce a data range that is centered around zero, so that the modified range is $[-128, 127]$. This step reduces the dynamic range requirements in the DCT processing stage that follows. The DCT temporarily increases the bit-depth of the data, since the DCT coefficients of an 8-bit/component image take up to 11 or more bits (depending on fidelity of the DCT calculation) to store. This may force the codec to temporarily use 16-bit bins to hold these coefficients, doubling the size of the image representation at this point; they are typically reduced back to 8-bit values by the quantization step. The temporary increase in size at this stage is not a performance concern for most JPEG implementations, because typically only a very small part of the image is stored in full DCT form at any given time during the image encoding or decoding process. The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images [9].

Fig 3: Final configuration image

V. Security Analysis

Under our assumption of semi-honest parties, the security of the protocol depends solely on how much information Alice and Bob can learn from the data they receive during the process of the protocol. Let's review Algorithm 5 and 6. Alice received h1 = The from Bob, and Bob received X2 = XwR from Alice. To satisfy our QIT security model, by DEFINITION 3 and DEFINITION 4, it is enough to show that ∀Xw ∈ Rn×m, ∃X′w ∈ Rn×m, where Xw and X′w are QIT indistinguishable under the mapping function R, which is true iff R are noninvertible. Yet on the other hand, we need also to have T be to noninvertible to make the protocol QIT secure. The property of T to be rank deficient, however, makes the statement automatically true, i.e. it is always QIT secure for Bob. For any 1-D discrete signal x(u), and a given filter h(v), let the matrix after reformatting x(u) be Xu ∈ Rn×m1 and the vector form of h(v) be hv ∈ Rm×1. Then, the 1-D linear convolution can be written into a matrix product form as

$$y = Xuhv.$$

THEOREM 1. *Let $\gamma_1, \gamma_2, \cdots, \gamma_d$ be d random numbers, and*

$$L = \text{span}\left(\begin{bmatrix} 1 \\ \gamma_1 \\ \vdots \\ \gamma_1^{m-1} \end{bmatrix} \begin{bmatrix} 1 \\ \gamma_2 \\ \vdots \\ \gamma_2^{m-1} \end{bmatrix} \cdots \begin{bmatrix} 1 \\ \gamma_{\lfloor \frac{m}{2} \rfloor} \\ \vdots \\ \gamma_{\lfloor \frac{m}{2} \rfloor}^{m-1} \end{bmatrix}\right) \in \mathbb{R}^{m \times d}.$$

Let $x(u)$ be any 1-D discrete signal and X_u be the matrix reformatted from $x(u)$ as in Equation 5.1. If $R \perp L$, then $f(X_u) = X_u R$ is noninvertible for X_u.

VI. Conclusion

In this paper, a simple and strong method has been proposed for image security using a combination of block based image transformation and encryption techniques. The cases showed that the correlation was decreased when the proposed algorithm was applied to them before the RS algorithm. Experimental results of the proposed technique showed that an inverse relationship exists between number of blocks and correlation, and a direct relationship between number of blocks and entropy[13]. To learn mapping relations between image spaces, we perform parametric regression within small subsets of training image patch pairs. To this end, we propose a space partitioning scheme

that can divide the high-dimensional but sparse feature spaces into easily retrievable local clusters. For any test image patch, our method can efficiently retrieve its closest local cluster and perform regression within the cluster. We applied our framework to intrinsic image estimation and super-resolution and obtained state-of-theart performance. Compared with the two existing classical cryptographic security models, namely Information Theoretic Security and Computational Security, our proposed model provides less security than the former model in the information sense while enable us to develop protocols that are significantly faster than those under the latter model. The rigorous analysis of the security of the protocols for both parties was also presented. The experimental results showed that our pro- posed protocols improved the computational time largely. While there is some potential insecure point in our proposed protocols as is dis-cussed in Chapter 6, we need further improvement and analysis in the future. Other future work includes extending the QIT framework to more signal and image processing algorithms.

References

[1] A. Hertzmann, C. Jacobs, N. Oliver, B. Curless, and D. Salesin, “Image Analogies,” Proc. ACM Siggraph, 2001.
[2] Z. Liu, Z. Zhang, and Y. Shan, “Image-Based Surface Detail Transfer,” IEEE Computer Graphics and Applications, vol. 24, no. 3, pp. 30-35, May/June 2004.
[3] S. Bae, S. Paris, and F. Durand, “Two-Scale Tone Management for Photographic Look,” Proc. ACM Siggraph, 2006.
[4] W.T. Freeman, E.C. Pasztor, and O.T. Carmichael, “Learning Low- Level Vision,” Int’l J. Computer Vision, vol. 40, pp. 25-47, 2000.
[5] J. Besag, “On the Statistical Analysis of Dirty Pictures (with Discussion),” J. Royal Statistical Soc., Series B, vol. 48, no. 3, pp. 259- 302, 1986
[6] S. Baker and T. Kanade, “Limits on Super-Resolution and How to Break Them,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 9, pp. 1167-1183, Sept. 2002.
[7] M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS’02, Ghent, Belgium. *Proceedings of Advanced Concepts for Intelligent Vision Systems*, 2002.
[8] S. Changgui, B. Bharat, "An efficient MPEG video encryption a lgor i thm, " *Proc e edings of the symposium on reliable distributed systems, IEEE computer society Press*, 1998, pp. 381-386.
[9] S. Fong, P.B. Ray, and S. Singh, "Improving the lightweight video encryption algorithm," *proceeding of iasted international conference, single* processing, pattern recognition and application, 2002, pp. 25- 28.
[10] S. P. Nana'vati., P. K. panigrahi. "Wavelets: applications to image compression- I,". *joined of the scientific and engineering computing*, vol. 9, no. 3, 2004, pp. 4- 10.
[11] c. Ratael, gonzales, e. Richard, and woods, "Digital image processing," 2nd ed, Prentice hall, 2002.
[12] M. Yuan and Y. Lin, “Model Selection and Estimation in Regression with Grouped Variables,” J. Royal Statistical Soc. Series B, vol. 68, pp. 49-67, 2006.
[13] V. Roth and B. Fischer, “The Group-Lasso for Generalized Linear Models: Uniqueness of Solutions and Efficient Algorithms,” Proc. 25th Int’l Conf. Machine Language, 2008.
[14] P. Tseng and S. Yun, “A Coordinate Gradient Descent Method for Non smooth Separable Minimization,” Math. Programming Series B, vol. 117, pp. 387-423, 2009.
[15] K. Huang and S. Aviyente, “Sparse Representation for Signal Classification,” Proc. Advances in Neural Information Processing Systems, vol. 19, pp. 609-616, 2007.
[16] M. Aharon, M. Elad, and A.M. Bruckstein, “The K-SVD: An Algorithm for Designing of Over complete Dictionaries for Sparse Representations,” IEEE Trans. Signal Processing, vol. 54, no. 11, pp. 4311-4322, Nov. 2006.
[10] S.S. Maniccam, N.G. Bourbakis, "Image and video encryption using SCAN patterns," *Journal of Pattern Recognition Society*, vol. 37, no. 4, pp.725–737, 2004.

.