IMAGE ORIENTATION BASED WATERMARKING TECHNIQUE IN COPYRIGHT PROTECTION

HEND MUSLIM JASIM, ZAITON MUDA, MOHD TAUFIK ABDULLAH
Faculty of Computer Science and Information Technology
Putra Malaysia University, Malaysia
E-mail: [1]hend_muslim1974@yahoo.com, [2]zaitonm@upm.edu.my, [3]mohd@upm.edu.my

ABSTRACT

As a means of copyright protection, the use of watermarking has still not reached a significant level of reliability in applications to resolve infringement claims in the courts. This is because of two main obstacles. The first raises the need to consider original image quality as the main evidence over any other clues whereas the second denotes the lack of an adequate common measure that prove the superiority of one technique over another and then prevent improvement on efficiency and quality of algorithms. In seeking to address this problem, this research proposes a new image orientation watermarking technique based on the possession of the highest quality of the original image as the main evidence in copyright disputes and proposes a generic measure capable of scoring the performance of the different proposals. This design benefits Principal Component Analysis and Blind Noise Level Estimation to resemble a set of image transitions over resizing operations in response to owner signature. To deduce copyright, watermarked image besides its original coordinates are incorporated in copyright issues with the aid of two formulated parameters; Protection Requirement (PR) and Distance Decision (D) that are to serve as a protection requirement measure and a resolving parameter respectively. The design along its obtained results shows convincing validity results that are further explicated using ANOVA and linearity testing.

Keywords: *Digital Right Management Techniques, Image Copyright Protection, Watermarking Principal Component Analysis, ANOVA*

1. INTRODUCTION

Image copyright protection utilizes watermarking as one of the different Digital Right Management (DRM) techniques to secure digital images [1, 2].
The use of watermarking has still not reached a significant level of reliability in copyright protection applications to resolve infringement claims in the courts [3]. This is because of two main obstacles. The first involves the need to consider original image quality as the main evidence over any other clues and the second involves the lack of an adequate common measure that proves the superiority of one technique over another and then prevents improvement on the efficiency and quality of algorithms. Watermarking is used to conceal information over long time frames and emulates steganography which is a process of hiding secret messages, and is the basis of any operation in any given cover letter following an algorithm [4]. Research has pointed to the value of steganography in providing copyright protection for digital products. In this application, steganography is known as watermarking and its main activity of hiding is defined as "embedding." Watermarking involves embedding and extracting in which a signature is concealed and collected, respectively, in two different stages of operations. This distinction in the terminology differentiates the embedding process from that of the hiding activity such that the former is not necessarily invisible while, in the latter, the whole function relies on the capability of concealing messages within a cover and where the element of invisibility must be present [4]. The main challenge in watermarking is to balance watermark visibility and robustness [5], and its performance against a set of watermarking requirements is the primary aim of techniques that are developed and used. Watermarking in signature embedding is unable to comply completely with the requirements of consistency, as it is difficult to satisfy them all simultaneously [6]. In addition, it is impossible to avoid data change during the process of embedding a signature into it.

This research attempts to model a new watermarking strategy in image protection systems by using original image quality features as the main part of evidence instead of its signature and to propose an adequate common measure to compare between the different techniques. So far, signature has been treated as a primary key in most of proposed techniques. Here, signature constituents are used to stimulate a sequence of operations on the image rather to be embedded. The work invokes ANOVA and regression residual testing to support validation of the obtained results drawn from the main procedure in the designed technique.

2. PRIORITIES IN PROTECTION TECHNIQUES: FROM TEGANOGRAPHY TOWARDS WATERMARKING

While there have been many trends on image copyright protection, steganography techniques have drawn much attention and have rapidly developed into a completely different application discipline. Unlike watermarking, steganography involves the practice of undetectable communication of a message in a cover letter by exploiting its capacity [7]-[9]. Similar to watermarking, its modern definition addresses digital images, audio, video, and in documents. In general, the basis of the main functions in watermarking and steganography, which is to hide information, seems to be similar although there are some slight differences.

Technically, in distinguishing between the two, the main criteria employed by most researchers are on requirements. In particular, the robustness of the hidden message along with its cover is referred to as watermarking. Copyright protection requires the message to accompany the cover under all expected conditions whereas in steganography, the priority is on security in addition to the robustness [10]. However, when it comes to the matter of goals and objectivity in the two techniques, neither robustness nor security are crucial in differentiating each other; instead the capacity requirement characteristic emerges as the best in distinguishing between the two. The main obligation of watermarking is not towards imbedding a huge size of owner signatures but lies in the possession issue which runs better with smaller size and avoiding a corruption of the hosting cover [11]. On the other hand, steganography awareness is on the hidden message, and capacity is then a requisite [12]-[13] with the greater capacity offered on the hidden information defining the efficiency of the technique. More generally, the difference between steganography and watermarking is on the priority between the concealed message and the cover letter. Some, such as [14] uses the term importance to point out this fact. The soundest conclusion is that in steganography the priority is on the hidden message over the cover letter whereas in copyright protection it is on the cover letter. Consequently, to remove any vagueness, the techniques of steganography can be identified as message oriented and that of watermarking as cover oriented. Inevitably, there is a serious ambiguity in requirements that characterizes both watermarking and steganography to cause a mix-up for most trends to satisfy. Besides, there are a number of key requirements for each technique to be deemed efficient that are often contradictory to each other [15, 16].

In the attempt to remove this ambiguity, this research uses the term orientation to distinguish between the two techniques, (see Figure 1). There are serious considerations on information and data exchange in addressing the ambiguity between the two. In steganography, information denotes the secret message that utilizes image data as a cover. However, in this message, the signature is not the main concern and thus does not denote the real information in watermarking where the image is the focus even though techniques highlight the signature. As such, instead of getting the orientation focused on the image, signature orientation overrides all the proposals in copyright protection matters.

3. LITERATURE REVIEW

Watermarking techniques have been classified into two main approaches; the Spatial Approach and the Transformational. In the first, the signatures directly change the original (cover) image's intensity based on a set of given rules of the designed algorithm. This mode requires simple and low computing complexity because no other transformation is experienced. Most of the devised algorithms have used the Least Significant Bit (LSB) of the cover to resemble the signature data. The difference between those works may address different objectives such as how to embed, limits of embedding size, and type of the cover space colour used to host the watermark. [17] used LSB spatial embedding supported by a Discrete Cosine (DCT) transformation in the watermarking technique. This work applies a Gabour filter to enhance image quality after the extraction process. [18] also used LSB embedding, but this technique goes further to host multiple watermarks with the watermarking. Researchers combined the MSBs of the watermarks before they embed them into the LSB of the cover to improve the watermark's invisibility. [19]

employed the green channel of the color space of the cover letter in this watermarking technique.

The second watermarking approach is named transformational because watermarking embeds the watermark into the transformed copy of the image rather than in the original. Usually the presented works in this approach use frequency-based transforms such as Discrete Wavelet (DWT), Discrete Fourier (DFT), and Discrete Cosine (DCT). Analytic approaches of matrices can also be taken in this category as the outcome still represents an alternative space to the spatial such as Singular Vector Decomposition (SVD). Although the transformational approach is more complex compared to the spatial, it compels diverse applications in literature. [20] modelled the Eigenvalue quantization of the DWT in a watermarking technique to strengthen robustness against attacks as the main destination. [21] used DWT and SVD for the main objective while [22] watermarked audio media cover by making use of the remaining numbers in DCT. Their goal was to achieve a good trade-off among transparency, robustness, and capacity being aware that watermarking requirements have different control disciplines. [23] applied watermarking on gray scale images without affecting the imperceptibility in his oeuvre. [24] sought to overcome different approaches by combining SVD, encryption and DWT in their technique. Although the transformations in the different techniques seem alike, there are however many goals characterizing each over the other. [25] discussed the advantages of DWT multi resolution characteristics as a justification to depend on watermarking. This work sought to prove a good robustness against image common operations like JPEG compression, cropping, and sharping, and contrast adjustments in this technique. [26] used SVD to stand against image operations. [27] improved the invisibility of watermark using DWT, and [28] by combining DWT and SVD, achieved good levels of inaudibility and robustness in reliable music business, while [29] combined DWT and DCT in the presented technique. The experiments of this work are outstanding in different image operations. Interestingly, [30] developed an adaptive technique along DCT to show a non-static methodology in watermarking as another approach to succeed.

4. WATERMARKING ORIENTATIONS

This research sought new criteria to classify watermarking algorithms away from the existing classifications. Because of the close relationship between steganography and watermarking, the main goal of the classification is to target the orientation of the watermarking. This research proposes a new concept in classifying watermarking techniques. When the evidence targets signatures, the whole operation is most likely to be termed as signature oriented. Whereas when the evidence is made to target the quality of originality in the specifications of images, watermarking is deemed to be image oriented. On this classification basis, it is possible to identify the main orientation of watermarking as to whether it addresses the cover letter or the hidden message or clarifies the differences between steganography and watermarking. Mostly, it is difficult to disregard the main function of protection to hide data in a cover letter when it comes to signature under conditions of accompanying it with the image. However, it is fairly simple to point out the orientation of the hiding function towards evidence-based decision-making objectives. When it prioritizes the original image over the signature, watermarking becomes image orientated and when it focuses on the signature it is signature orientated. In other words, the classification specifically addresses the extraction procedure and does not focus on the embedding mechanism. Unlike the usual approaches, the main perspective sought is on the way of changing the image data in accordance with signature pixels value, whereas in the orientation-based classification the clue to approving ownership determines the orientation towards the signature or to the image.

Whether the technique is spatial or transformational, all styles in the presented literature review are classified as signature oriented where the main targeted clue of ownership is the signature. The effort in this orientation does not focus on rigid clues such as image quality and original specifications but implicitly declare that ownership is thoroughly dependent on the existence of owner signature only and discards any other withstanding evidence. Therefore, when a watermarking technique fails to extract a signature, the protection also fails. In addition, copyright in signature-oriented whereas watermarking depends crucially on the security of the algorithms. When hacking an algorithm, the protection no longer exists.

5. PROTECTION SYSTEM DESIGN

The strategy of protection in the proposed technique relies on the original image as the main evidence of ownership. As such, the system acts to generate a copy of that original in order to deploy it to the public without avoiding any fraud while leaving the original safe. Technically, the system acts to move the image from its presumed original location to a pre-determined deviated position in a space. Consequently, alleged claims are able to access and use the deviated copy but not the original. This can be re-formulated to be clearer by suitable definition using relative measures over the separating distances. In Figure 2, the original image is located at Pos, and the deviation process shifts it to Pof. Any alleged copy would then be located somewhere around Pof, say Pas and certainly not close to Pos. When measures are used, distance comparisons would yield which locations are closer to each other, i.e., the original ending Pof to the alleged starting Pas or alleged ending Paf to the original starting Pos. Logically, the measure that satisfies the minimum distance nominates the configuration of original starting image ahead of the alleged over the alternative, i.e., Doa over Dao.

This absolute comparison of distances in this manner is computationally costly because of the need to rotate a set of vectors in multi dimension space [30] together with conducting the PCA technique for image projection. The PCA technique analyses a set of given vectors and factors them such that each becomes a combination of a set of fundamental coordinates associated with corresponding projections. The terminology uses scorings and loadings in this context to distinguish the first set from the second for the coordinates and the projections respectively.

In case of absolute comparison, a process to unify the loadings of the two configurations is required to reference only one set of vectors in common by rotating the loadings of one of the two configurations to the other. Therefore, the mean location is used as an alternative resolve. This view confirms that the deviated copy is far from the original. Any additional corruption introduced into this copy would not drift it away more. This, in fact, reflects the main principle of the whole process of copyright decision-making adopted in this design. This process assumes two random configurations of tracing paths, selecting one image at a time as a starting point along multi transitions path of resizing operations controlled by concatenation items of two signatures - one corresponding to the image followed by the second signature ending up with a final point. Obviously, the configurations differ from each other by their starting images used to initiate the tracing path and the sequence of concatenating signatures of owners. Let us assume that we have an original image and an alleged one; thus we have an owner signature and an alleged one as well. Then there are two tracing path configurations to consider. Arbitrarily one of the two images is the starting image and correspondingly the concatenation of the signature comprises the related signature first followed by the second. On the other hand, the second tracing path is configured by the other image and its signature is set forth in the concatenation of the two signatures. However, tracing layout can be extended to cover multi-claim configurations where paths considered should cover all the possible sequences of the involved images and their signatures. Formally, the two configurations can be defined with the aid of Figure 3, as follows:

Claim one: owns image 1 and attributed by signature 1 $_{\text{character 1.. character n}}$

Claim two: owns image 2 and attributed by signature 2 $_{\text{character1..character k}}$

The configurations constructed are:

Configuration one:

image 1 traced along signature concatenation< signature 1- signature 2>$_{\text{character 1 .. Character n+k}}$

Configuration two:

image 2, signature concatenation < signature2- signature 1>$_{\text{character 1..character k+n}}$

Recall the main principle stated earlier where any additional corruption made onto a corrupted copy would not drift the location away more from the original. In other words, the mean location of all image copies corrupted has to be distantly apart from their original. With this fact, the decision-making process settles the final resolve by the comparison between D1 and D2 such that:

Image i is original if corresponds to the greater Di

Where

Di = | Pstarting image – Pmean position of all images | (1)

Taking that into consideration, D is the distance measured between the starting point of the image used in a configuration to the mean position of all image copies generated in this configuration following the concatenation of signatures.

Image i, signature concatenation < signature i -signature j>$_{\text{character 1..character k+n}}$

5.1 Procedure One (Watermarking)

The block diagram of Figure 4 depicts the different functions of the watermarking procedure as a system. In this procedure, an image and a signature are required as inputs and the related output is the watermarked copy of that input. Signature constituents are indexed to stimulate a sequence of image operations using resizing only in different settings; resize ratio and number of times to impose. Final stage in this procedure computes the PR parameter, which is expressed in relation (2), to decide the validity of the protection by a threshold identifier under PCA analysis scheme and a blind estimate of noise measuring that is depicted in Figure 5. If the computation scores a value lower than this threshold, signature has to be changed in return to meet the threshold specification.

5.2 Procedure Two (Copyright Infringement Resolve)

The block diagram in Figure 6 shows the different units constructing the data manipulation in the second procedure of this system. In this procedure inputs are a pair of claims each presents an image and related signature. The output nominates the original over the alleged copy relying on comparison process between two Distance Decision parameters (D^1 and D^2) as in relation (1). The core activity of this procedure relies on the processing of image and signature data and the means to construct PCA analysis X matrix from copies of the images in row wise. This activity is already illustrated in Figure 5.

5.3 Protection Requirement Measure (PR)

Based on the design principles, each image is divided into a set of segments and their noise estimates are used to construct a row in a matrix known as X (Figure 6), which represents the input to PCA. The PCA factors this X matrix into a set of scoring and loading vectors. Interestingly, the more an image is corrupted, the greater its related noise estimates are scattered over distant locations away from the original. The original copy is the main evidence used to support owners' copyright approval. When a deployed copy is further away from its original in the PCA space, it is hard to reconstruct and return it to its original location with the aid of available digital filters and/or other image processing techniques [32, 33, 34, 35]. A necessary tradeoff is sought to maintain the corrupting noise on the one hand and to guarantee the success of the protection mechanism on the other. This tradeoff represents the main objective of the protection system and is expressed in terms of a formulated measure called the Protection Requirement (PR) assuming the fulfillment of the following constraint:

$$PR = \mathrm{Log}\,(D_{wi\text{-}org}/\,D_{org}) > \quad T \qquad (2)$$

Where, $D_{wi\text{-}org}$ is the distance between locations at the corrupted image and its master copy on PCA, D_{org} is the distance of original copy from the origin of PCA space, and T is a threshold evaluated empirically as a constraint for protection purposes.

This expression is derived from the logical requirement sought to protect an image. The more an image, or the consumer copy, deviates from its master copy, the more it is secured. In relying on this fact, PR considers two aspects in formulating equation (2). It gives the displacement distance between the two copies as a function of original position. The Log function is used to include sign reflects on measures such that when the displacement between the two copies becomes multiples of original, which is the case of the requirement, PR is positive and when those distances are comparably equal, the sign turns to negative alarming for undesired situations. The PR technically covers different scopes of signal-to-noise measurements. The derivation of the threshold T for PR has been inspired empirically from the unsuccessful attempts incurred where some experiments fail to protect images. Data on failures are collected and their associated measures reviewed. It is noted that no single measure is capable of classifying failed experiments from the successful ones or a combination of them depending on existing noise measures like PSNR, MSE, MAXERR nor L2RAT. The PR, with its conjugated threshold, efficiently classifies all the trends. As locations are functions of the measured noise, PR does not resemble only the signal to noise ratio but steps further to control the tradeoff between noise and the minimum distance necessary to keep the master image as safe as possible (see Figure 7). This measure of PR along with the threshold T is, in fact, a universal measure that is adequate for any comparison process among different proposals. However, investigations on the experiments along with the implementation of individual measures on signal-to-noise ratios are well demonstrated in the following section.

6. EXPERIMENTS AND RESULTS

Five different images are used in the experiments and a total of 2500 experiments were conducted in the testing section of system validation over PR. Experiments address two main featuring characteristics that is to approve PR's withstanding measurements in relation to the common measures used such as PSNR, MSE, MAXERR and L2RAT to estimate image noise status and to decide on protection validity. Therefore experiments have to confirm PR characteristic such that in Noise to Signature be functioning appropriately to monitor any change on image in comparison to other measures. Besides, PR has to be distinctively classify validity status of a given attempt in protection process. Towards these two conditions, experiments are divided into two levels; watermarking and infringement resolve, to confirm the two characteristics investigating PR features as an adequate evaluation measure within the general frame work of the proposed design, namely:

Level one is to define an operative relation correlating the length of the signature to the level of noise resulting from image resizing as a trend to determine a proper validity requirement for PR.

Level two is to show the effectiveness and validity of implementing PR as an adequate alert-control parameter in a copyright protection technique.

6.1 PR vs. Existing Measures on Signature to Noise Characteristics

On the design bed of the watermarking technique proposed in this work, a signature is used as a simulated sequence of data corruption operations that are determined by their constituents. Each signature has to have a distinct corruption result that, in turn, confirms the fact that each signature has to be a noise-based measureable variable. To formulate this behavior, the experiment was controlled in such a way as to take an image and corrupt its content by a signature. Signatures are ordered randomly in predefined subgroups according to their lengths. A group of two-element signatures (alphabetically comprising two characters, such as AR or SD) is followed by a group of three element signatures (such as ADE or KGO), and so forth. Measurement is then applied in each case to estimate the resulting noise incurred by the sequence of resizing operations predicted with all the available measures following their definitions in publications. The results are summed up by averaging the obtained estimates for all cases at each length category and then depicted in a single figure for viewing the characteristic of the signature length versus its corruption estimate. The less the scattering of these averages collected the more the dependency of suggested measure yields. Figures 8 is an example of the obtained results on one image. The behavior of all measures, namely, PSNR, MSE, MAXERR, and L2RAT beside PR are studied separately and given in a subplot. In this figure, there is a tagged table that shows the average calculations drawn from the experiments conducted at the first watermarking procedure as a summary. In this table, records are organized into five groups in according to signature length. Thus, there are five groups in each a set of experiments assigned to individual records. The average results of all record measurements falling into one group are summed up and divided by the number of records to give the final calculation aggregated in the records of a summary table provided at the lower right corner at each figure. These figures apparently allow for a crucial decision on the invalidity of the existing measures because they show anomalous behavior versus signature length when compared to PR. Although the main consideration is drawn as random behavior, the overall behavior of the measures except for PR points to the irregularity in regression, such that there is no quite definite rule controlling the variation as a systematic estimate. The expected conduct assumes the fact that when the signature length increases, the proportional noise measure also increases. In fact, there is no clear relationship that is able to explicitly describe this behavior either individually or by a combinatorial running on signature length. Besides, the behavior indicates that MAXERR and L2RRAT are reflective parameters of PSNR and MSE and, as such, are discarded from possible consideration in the investigation of the analysis and experiments discussed later. On the contrary, PR stands up efficiently to show linear alike correspondence to the underlined signature variations. Further investigations to confirm on this conclusion contribute rigid mathematical background employing statistical inference of ANOVA and regression residual testing.

ANOVA provides a statistical test of whether the means of those signature groups reflect adequate samples for a valid population behavior. In this context, the theoretical background of this test relies on a normal random distribution basis organized along different group sections of owner signature forming multiple distributions such that each group has its own x-coordinate and its Population Mean i, i=1 .. 5, as depicted in Figure 9. Signature lengths assigned are 2, 3, 4, 5, and 6 characters for the five groups numbered 1, 2, 3, 4, and 5 respectively. Equality is addressed as a criteria of variation among the population means of those groups using inference testing and enrolling sample means (sm i, i=1 .. 5) as inputs. For this test, there are two hypotheses, Ho and Ha, and ANOVA yields which of them to confirm. When Ho is confirmed, the conclusion is that the means of signature measures are all equal and thus there is no variation when it comes to characterize signature change. However, when Ho is rejected, that in turn means that there is a remarkable change. The extent of change is scaled according to a linear relation that is assumed with regression fittings. Therefore, further investigation on linearity is addressed.

The less the scattering of values around the assumed regression line, the more linear the signature is to its noise collected measures. The overall comparison of this study is summarized by the results provided in two folds, that is, ANOVA and sum of residual squares. Table 1 emphasizes the validity of PR over the other measures in the sense that it has the minimum resistance p estimates (P-value = 1.5E -150) against the rejection of Ho. A summary of all ANOVA tables obtained on each measure is given in Table 2. Each measurement in the table addresses each group separately from the 2-letter to the 6-letter group. At each record, statistical variables are computed denoting the count, sum, average, and variance of each measure distribution characterizing the table's identity. Each table is tagged to the inference measures that support the hypothesis of population inference or stands against it. The main P-value attribute dictates its superiority among the others to fully raise its minimum resistance against the rejection of Ho declaring the most variation of PR as a function of the signature length.

Table 2 Summary of ANOVA Comparison

P-value	**PR**	**PSNR**	**MSE**
	1.5E-150	1.34E-09	4.15E-07

For more on the linearity comparison, regression theory can be applied. Estimates of measures at each signature group are random distributions sketching their means to a single regression line extending at the mean values in each group with a variance. This test computes the residual, which points out the amount of scattering around the mean value of the estimate, at each signature group by subtracting the sample score from the mean value at the relevant group. Figure 10 on five images tested provides a clear view on the validity of PR thus obtained over the others in the sense that it has the minimum scattering around their regression lines (∑ Residuals2=18.364). This figure contains two plots for each measure involving the regression line fit and the residual plot depicting residuals at each behavior. The corresponding summary on the residual sum of the measures provided in this figure is given in Table 3.

Table 4 Comparison Summary of Linearity Residuals

$\sum$ Residuals^2	**PR**	**PSNR**	**MSE**
	18.364	1249	158116803.1

6.2 PR as an Efficient Requirement Controlling Parameter

By employing the protection system on images and separating the successful from the failed experiments, a trend is created to formulate an adequate classifier. The data in this level refers to data collection based on the run of infringement resolve experiments that is, watermarking followed by the infringement procedure.

The experiment on infringement resolve requires a pair of claims feed with each claim enclosing an image and a signature. The attributes D1 and D2 are computed from each experiment on two given images and two signatures using relation (5). In fact, a simulation process is done to achieve preparation of the two claims in priori. The process of considering the watermarking original first, and then accessing the watermarked copy as an alleged original in another claim processing, acts to modify the content in obtaining the alleged claims requirements. In this experiment there is no need to group results based on signature length as was done in the first experiment. Instead, the records of the experiment have to be classified as being valid or not. The valid group comprises all experiments that satisfy the protection principle given in relation (1) having an original $D_{original}$ greater that D_{claim} associated with the alleged claim and, conversely, the invalid group consist of those not satisfying this principle where $D_{original}$ is less than D_{claim}.

A fairly similar deduction is arrived at from the first experiments of the watermarking procedure; there is no exact behavior that matches the goal of having proper controlling protection on protection validity with any noise measure except that for PR. By interpreting the logical function of the corruption process and the manner in which the customer copy deviates from the original, PR is expressed as in relation (2). The effectiveness of PR as an adequate classifier can be well described in terms of the characteristics studied in all experimental images and depicted in Figure 11 where valid experiments are stained blue and invalid ones red. PR against PSNR and PR against MSE are pairs of same experiment plots drawn to show the superiority of PR over its opponent. Clearly no exact value can be judged on measures like PSNR or MSE to discriminate among experiments validity. The only measure having efficient discrimination in comparison to the two is PR that emerges with its sharp threshold T. Both measures scan a wide range of values (the vertical spread) with no limits specifying the invalid experiment (red points). On the contrary, there is a clear threshold separator determined by PR (the horizontal spread) to categorize the two on their validity of protection status. A definite classification is obtained with a PR threshold value of T=0.05, which is experimentally determined to be an excellent classification completing the requirements stated in relation (2), as PR = Log ($D_{wi\text{-}org}$/ D_{org}) > 0.05 is the final step in the modelling aspect of the common measure proposed in the technique of this work.

7. CONCLUSIONS

Watermarking is used to protect images by embedding the owner's signature into image content. The validity of the protection is governed by a set of requirements. Despite the techniques used in embedding, watermarking should comply with the complete set of requirements applied together. The literature shows that the differences in implementing spatial and transformational techniques all act in the same manner when copyright is attributed to an embedded signature. All the techniques used in watermarking show it is a function of the algorithm used or to some other keying factors, and when these factors are known the images are no longer protected.

Watermarking involves a set of obligations namely, perceptibility, robustness, integrity, accessibility, compatibility, traceability, and security, although it is not possible to achieve high scores for all these requirements simultaneously. While watermarking involves embedding a signature by altering the image data, it tends to keep its quality as high as possible provided no changes are made. This contradiction between robustness and perceptibility set out as major goal in most publications.

While both watermarking and steganography have the common purpose of hiding data and embed messages in a cover, they each satisfy two different designated objectives. Watermarking uses the message to protect the cover by focusing on the image rather than the signature. Steganography, on the other hand, uses the cover to deceive intruders from accessing the embedded message and as such the priority is to the signature over the image. This confusion has led some calls for including an additional requirement such as the capacity to address some watermarking proposals and to discard it in some other works.

In brief, the contradiction on using watermarking as a tool in image protection is the basis for proposing an alternative design for such protection in this research. The proposed watermarking technique intentionally corrupts an original image under its owner signature in issuing a customer copy. Unlike existing techniques, the proposed technique does not hold the owner's signature as paramount; instead the customer's image is made traceable by its owner's signature by explicitly embedding it in the image. Corruption utilizes image resizing operations to come up with an intrinsic and a systematic data change. Finally, the proposed technique formulates two controlling parameters, namely PR protection requirement, and D infringement resolution to provide successful protection and to resolve copyright issues respectively. Experiments on PR characteristics show the performance on two levels of achievements regarding Signature to Noise Characteristics and its functional threshold alerting validity of protection with a threshold of 0.05.

REFERENCES

[1] Gaurav N Mehta, Yash Kshirsagar and Amish Tankariya, "Digital Image Watermarking: A review", International Journal of Scientific Engineering and Technology, Volume No.1, Issue No. 2, (2012), pp: 169-174.

[2] Anthony Ciolli," Lowering the Stakes: Toward a Model of Effective Copyright Dispute Resolution", West Virginia Law Review, Volume 110, No. 3, (2007).

[3] Maurice Schellekens, (2011),"Digital Evidence and Electronic Signature Law Review", Vol 8 Pario Communications Limited, http://sas-space.sas.ac.uk/5364/1/1965-2793-1-SM.pdf

[4] Manoj Kumar Sharma and P.C. Gupta, "A Comparative Study of Steganography and Watermarking, IJRIM, Volume 2, Issue 2, (2012).

[5] Ingemar J. Cox, Matt L. Miller and Jeffrey A. Bloom, "Watermarking Applications and Their Properties", Int. Conf. on Information Technology'2000, Las Vegas, (2000).

[6] Ravi K, Sharma, and Steve Decker, "Practical Challenges for Digital Watermarking Applications", IEEE Fourth workshop

Multimedia Signal Processing, pp: 237-242, Cannes, (2001).

[7] Shuliang Sun," A New Information Hiding Method Based on Improved BPCS Steganography", Hindawi Publishing Corporation Advances in Multimedia, Volume 2015, (2015).

[8] C.P.Sumathi, T.Santanam and G.Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding ", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, (2013).

[9] Eric Cole, "Hiding in Plain Sight: Steganography and the Art of Covert Communication ", Wiley Publishing, Inc., Indianapolis, Indiana, USA, (2003).

[10] Kutter, M. and Hartung, F.,"Introduction to watermarking techniques". In Information hiding Techniques for teganography and digital watermarking F.A.P. Petitcolas & S. Katzenbeisser (Eds.), (1st ed., pp. 97-120). Boston, MA: Artech House, (2000).

[11] Lalit Kumar Saini and Vishal Shrivastava," A Survey of Digital Watermarking Techniques and it's Applications", International Journal of Computer Science Trends and Technology (IJCST), Volume 2 Issue 3, (2014).

[12] Jeremiah Harmsen and William Pearlman, "Capacity of Steganographic Channels, IEEE Transaction on Information Theory,Vol. 55, (2009), pp. 1775-1792.

[13] Shamim Ahmed Laskar and Kattamanchi Hemachandran," High Capacity data hiding using LSB Steganography and Encryption, International Journal of Database Management Systems (IJDMS) Vol.4, No.6, (2012).

[14] Chun-Shien Lu,"Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property", Idea Group Publishing, (2005).

[15] Christine Podilchuk and Edward J. Delp,"Digital Watermarking: Algorithms and Applications", IEEE Signal Processing Magazine, (2001), pp. 33-46.

[16] Hai Tao, Li Chongmin ,Jasni Mohamad Zain and Ahmed N. Abdalla, "Robust Image Watermarking Theories and Techniques: A Review", Journal of Applied Research and Technology, Vol. 12, (2014), PP.122-138.

[17], Firoj Parwej,and Asif Perwej, "An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection" , The International Journal of Multimedia & Its Applications (IJMA) Vol.4, No.2, (2012).

[18] Subashini V J and Poornachandra S. , "A Blind Watermarking using MSB Insertion to Embed Multiple Watermarks", ICCCNT'12 26th_28th July (2012), Coimbatore, India.

[19] Abdallah Al-Tahan Al-Nu'aimi and Rami Qahwaji, "Green Channel Watermarking to Overcome the Problem of Multiple Claims of Ownership for Digital Coloured Images", International Conference on CyberWorlds, 7-11 Sep., (2009), Bradford, UK.

[20] M.A. Nematollahi,S.A.R. Al-Haddad, Faraneh Zarafshan ,"Blind digital speech watermarking based on Eigen-value quantization in DWT", Journal of King Saud University – Computer and Information Sciences, JKSUCI 141, (2014), PP. 10,

[21] Krishna Rao Kakkirala and Srinivasa Rao Chalamala, "Digital Audio Watermarking Using DWT-SVD and Secret Sharing" , International Journal of Signal Processing Systems Vol. 1, No. (2013).

[22] M. Mosleh and N. Hosseinpour, "blind robust audio watermarking based on remaining numbers in discrete cosine transform" International Journal on "Technical and Physical Problems of Engineering" (IJTPE), Issue 16, Volume 5, Number 3, (2013), pp. 18-26.

[23] Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Volume, 3, Issue 9, (2012).

[24] B. Pushpa Devi, Kh. Manglem Singh and Sudipta Roy," Dual Image Watermarking Scheme Based on Singular Value Decomposition", Trends in Innovative Computing - Information Retrieval and Data Mining, (2012).

[25] Kaushik Deb, Md. Sajib Al-Seraj, Md. Moshiul Hoque and Md. Iqbal Hasan Sarkar, "Combined DWT-DCT Based Digital Image Watermarking Technique for Copyright Protection", 7th International Conference on Electrical and Computer Engineering ,20-22 December, (2012), Dhaka, Bangladesh.

[26] Manjit Thapa, Dr. Sandeep Kumar Sood and A.P Meenakshi Sharma, ”Digital Image Watermarking Technique Based on Different Attacks”, (IJACSA) International Journal of Advanced Computer Science and Applications, Volume 2, No. 4, (2011).

[27] M.Mohamed Sathik and S.S.Sujatha, ”An Improved Invisible Watermarking Technique for Image Authentication”, International Journal of Advanced Science and Technology, Vol. 24, (2010).

[28] Ali Al-Haj and Ahmad Mohammad, “Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition”, European Journal of Scientific Research, Volume 39, No.1, (2010), pp.6-21.

[29] Mei Jiansheng, Li Sukang and Tan Xiaomei, “A Digital Watermarking Algorithm Based On DCT and DWT”, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA’09), , pp. 104-107 , Nanchang, P. R. China, May 22-24, (2009).

[30] Tao B. and Dickinson B., "Adaptive Watermarking in DCT Domain", Proc. Of IEEE International Conf. on Acoustics, Speech and Signal Processing, ICASSP-97, Volume 4, pp.1985-2988, (1997).

[31] David C. Lay, “Linear Algebra and its applications Fourth Edition”, Addison – Wesley, USA, (2012).

[32] Giachetti, A. and Asuni, N., “Real-Time Artifact-Free Image Upscaling”, IEEE Transactions on Image Processing, Volume 20, Issue 10, pp. 2760 – 2768, (2011).

[33] Rakesh M.R, Ajeya B and Mohan A.R, (October 2013),” Hybrid Median Filter for Impulse Noise Removal of an Image in Image Restoration”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 10.

[34] Shrinkage Kaikai Song, Qiang Ling, Zhaohui Li and Feng Li, “An Improved MRI Denoising Algorithm based on Wavelet Shrinkage”, 2014 26th Chinese Control and Decision Conference (CCDC), (31 May - 02 Jun 2014), Changsha, China

[35] Govind N Sarage, “Image Enhancement by Local Operators”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 1, (2015).

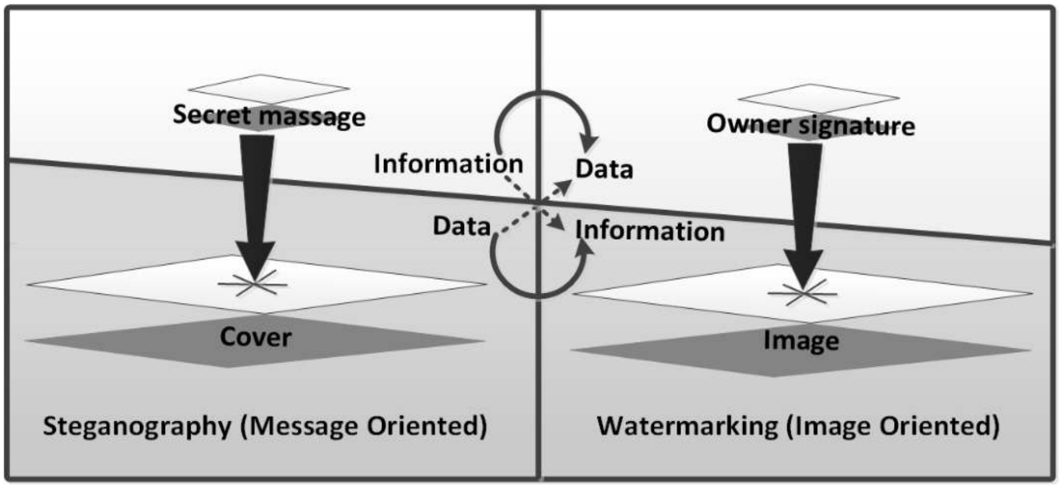


Figure 1. Main Distinction between Steganography and Watermarking

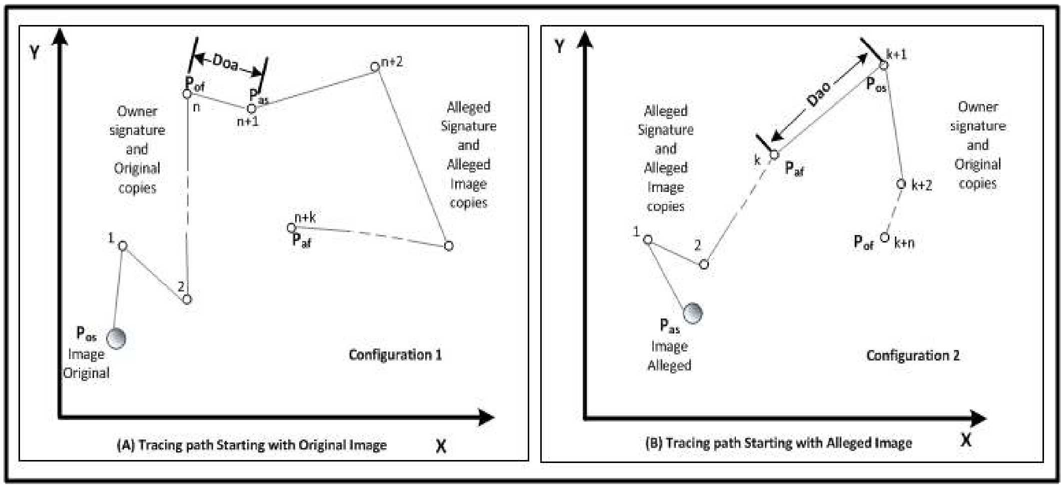

Y
Doa
P_of
P_as
n
n+1
n+2
Owner signature and Original copies
Alleged Signature and Alleged Image copies
n+k
P_af
1
2
P_os
Image Original
Configuration 1
(A) Tracing path Starting with Original Image
X
Y
Dao
k+1
P_os
Alleged Signature and Alleged Image copies
k
P_af
Owner signature and Original copies
k+2
1
2
P_of
k+n
P_as
Image Alleged
Configuration 2
(B) Tracing path Starting with Alleged Image
X

Figure 2. Theoretical Absolute Comparison Basis for Copyright Decision-Making

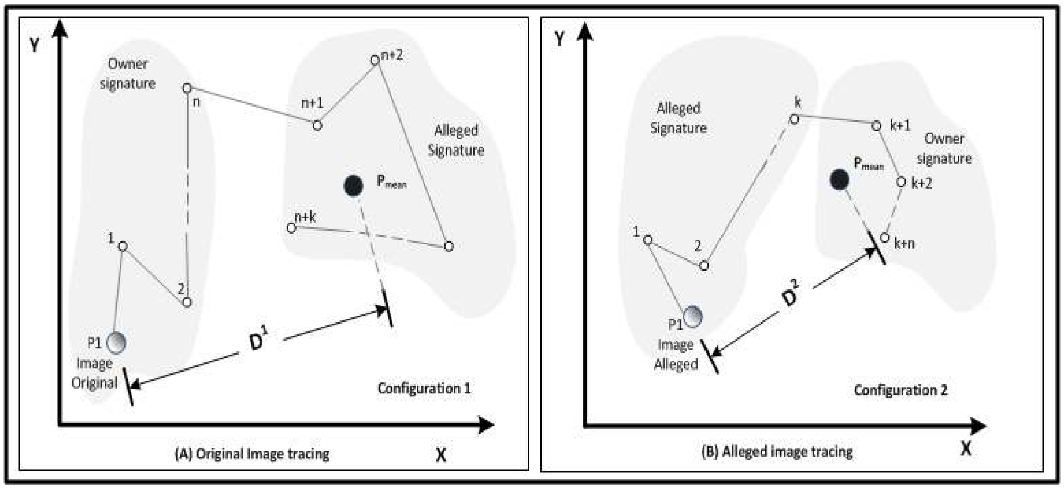


Figure 3. Principle of Image Protection

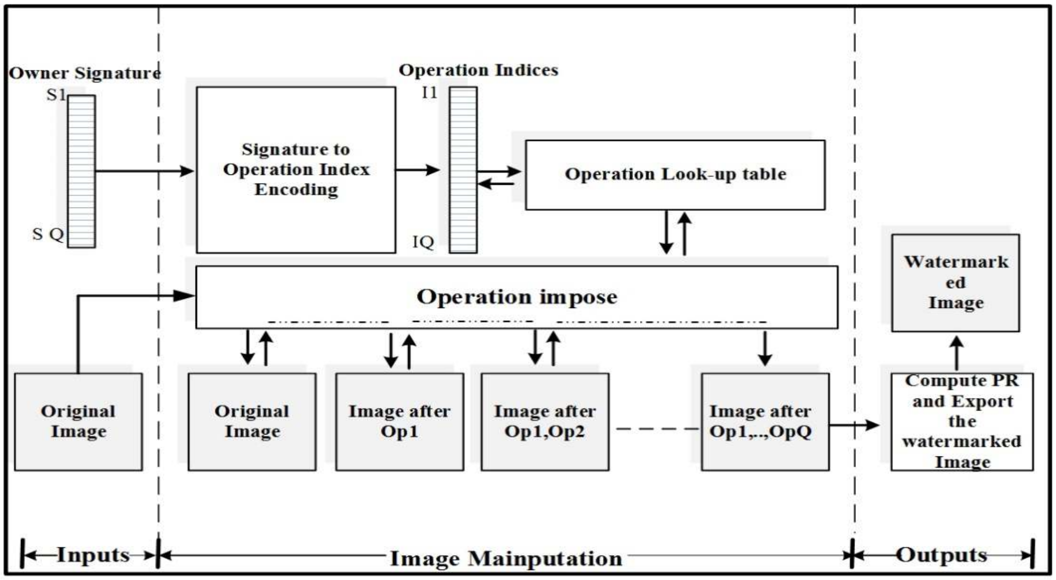


Figure 4. Procedure One-Signature Embedding (Watermarking)

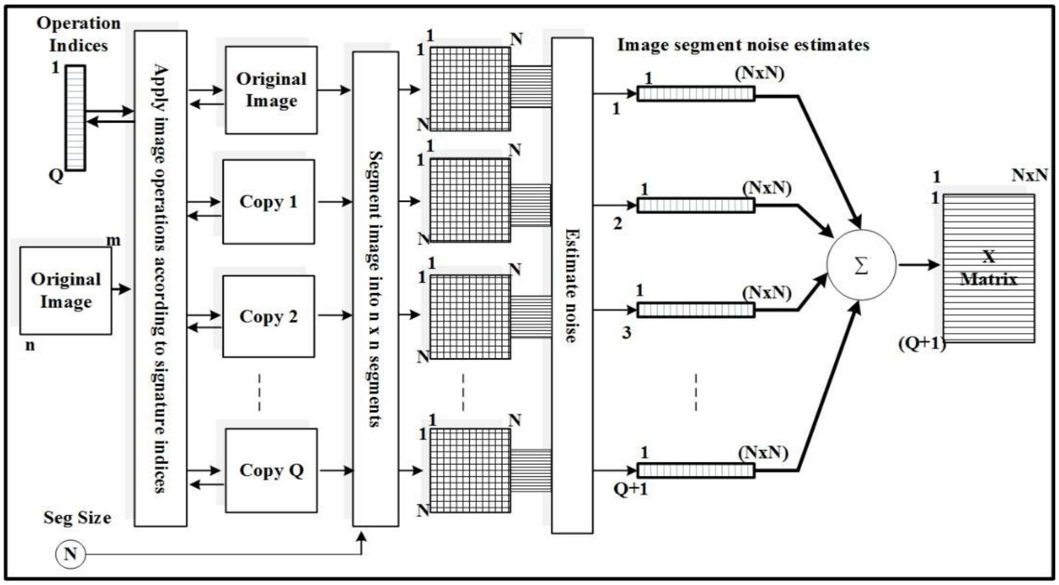


Figure 5: Applying Operations and Constructing X Matrix

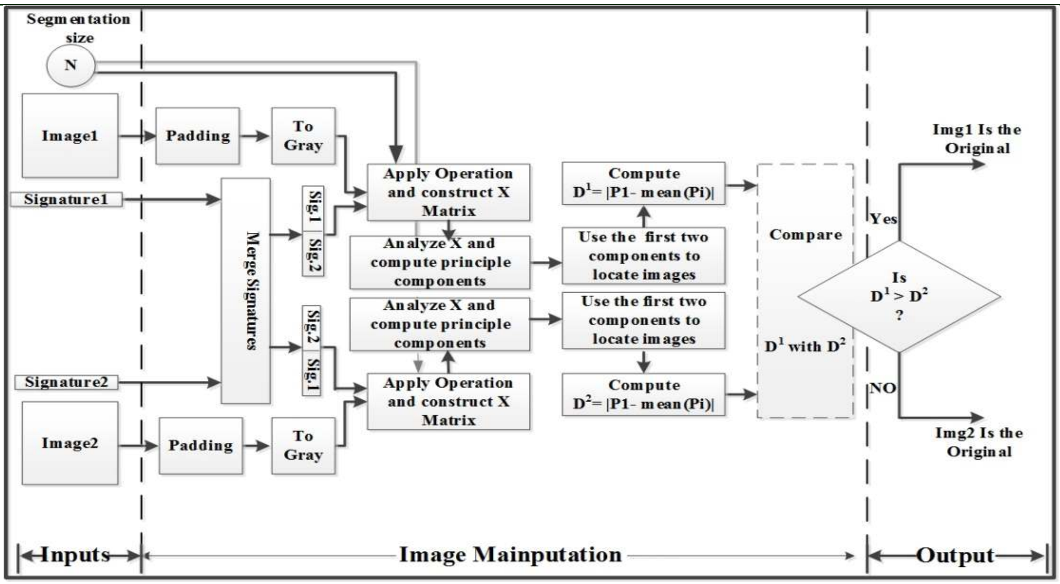

Segmentation size
N
Image1
Padding
To Gray
Signature1
Merge Signatures
Sig.1
Sig.2
Apply Operation and construct X Matrix
Analyze X and compute principle components
Compute D^1= |P1- mean (Pi)|
Use the first two components to locate images
Compare
D^1 with D^2
Yes
Is $D^1 > D^2$?
NO
Img1 Is the Original
Img2 Is the Original
Signature2
Image2
Padding
To Gray
Sig.2
Sig.1
Analyze X and compute principle components
Use the first two components to locate images
Apply Operation and construct X Matrix
Compute D^2= |P1- mean (Pi)|
Inputs
Image Mainputation
Output

Figure 6. Procedure Two: Copyright Infringement Resolve

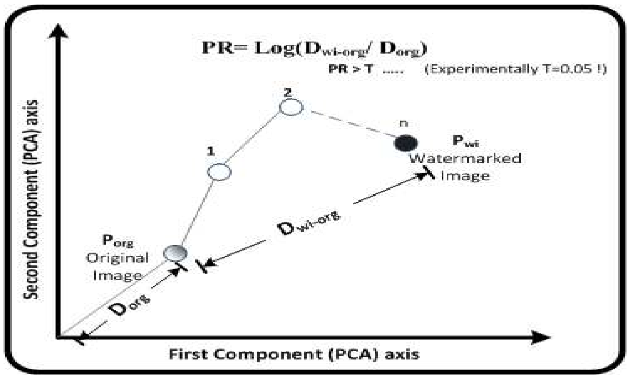

PR= Log(D_{wi-org}/ D_{org})
PR > T ..... (Experimentally T=0.05 !)
2
1
n
P_{wi}
Watermarked Image
P_{org}
Original Image
D_{wi-org}
D_{org}
Second Component (PCA) axis
First Component (PCA) axis

Figure 7. Noise-Based PCA Image Projection Space and Protection Requirement (PR)

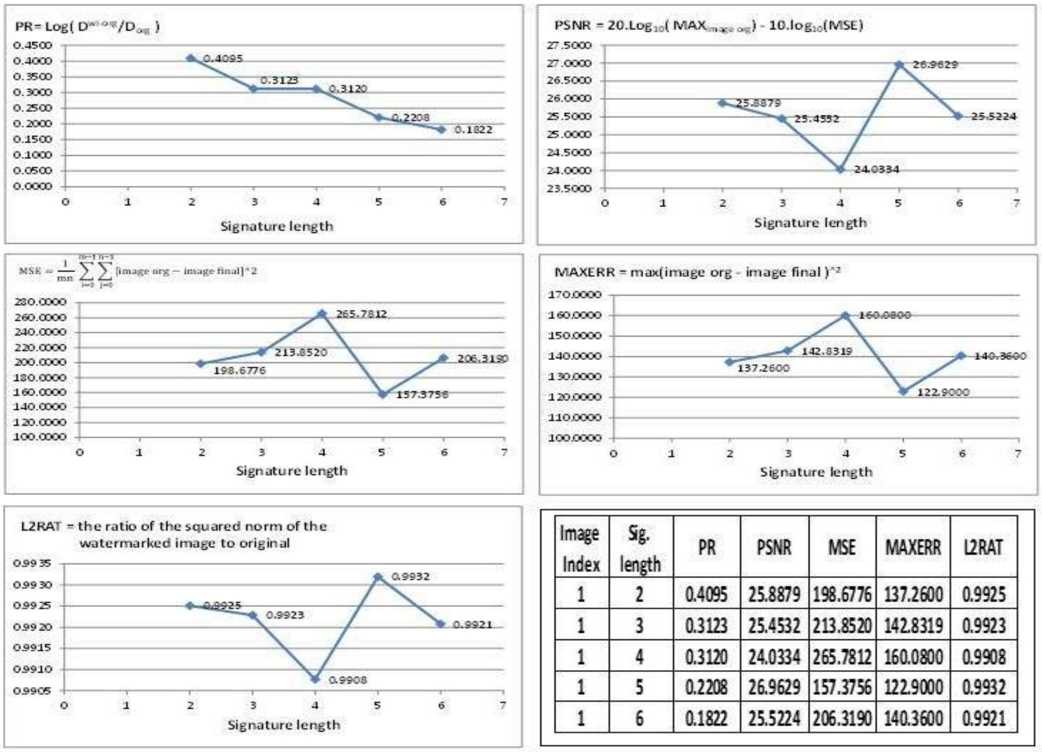


Image Index	Sig. length	PR	PSNR	MSE	MAXERR	L2RAT
1	2	0.4095	25.8879	198.6776	137.2600	0.9925
1	3	0.3123	25.4532	213.8520	142.8319	0.9923
1	4	0.3120	24.0334	265.7812	160.0800	0.9908
1	5	0.2208	26.9629	157.3756	122.9000	0.9932
1	6	0.1822	25.5224	206.3190	140.3600	0.9921

Figure 8. PR vs. Existing measures on Signature to Noise Characteristics

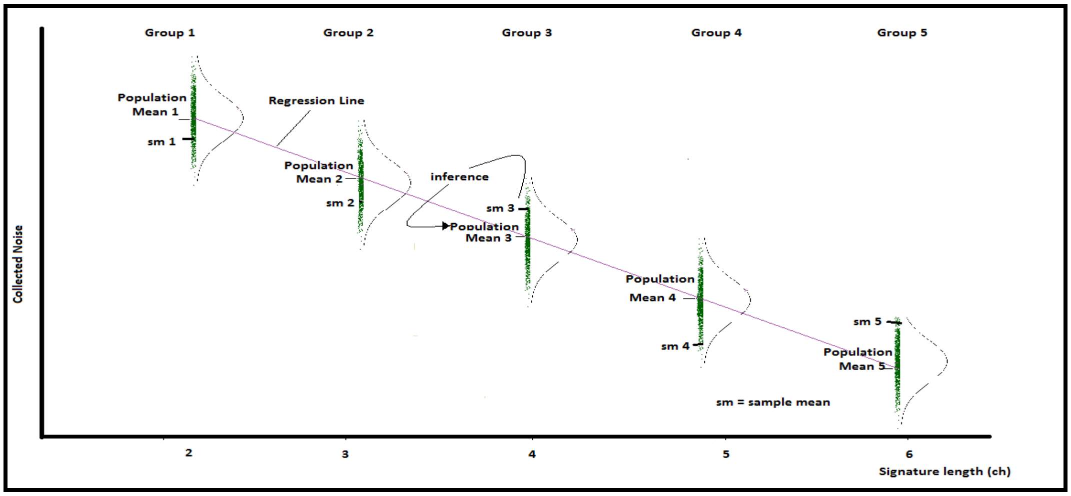
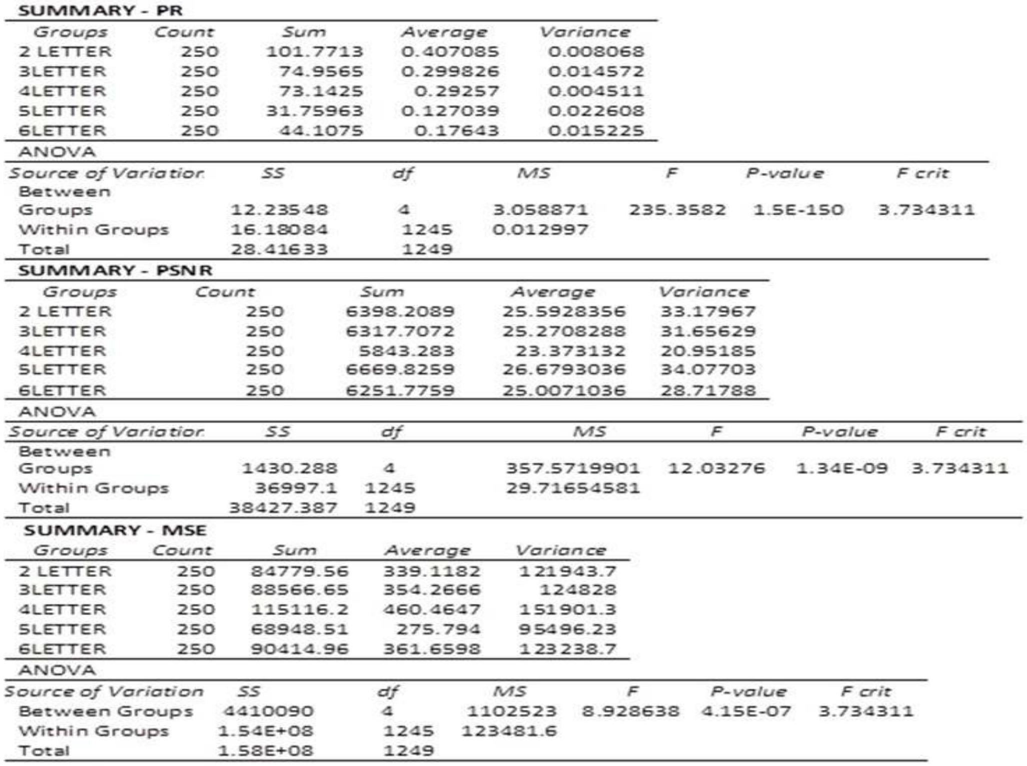


Figure 9. Theoretical Signature Length Based ANOVA Testing for Linearity

Table 1 Comparison of Measure Variance Analysis



SUMMARY - PR

Groups	Count	Sum	Average	Variance
2 LETTER	250	101.7713	0.407085	0.008068
3LETTER	250	74.9565	0.299826	0.014572
4LETTER	250	73.1425	0.29257	0.004511
5LETTER	250	31.75963	0.127039	0.022608
6LETTER	250	44.1075	0.17643	0.015225

ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	12.23548	4	3.058871	235.3582	1.5E-150	3.734311
Within Groups	16.18084	1245	0.012997			
Total	28.41633	1249				

SUMMARY - PSNR

Groups	Count	Sum	Average	Variance
2 LETTER	250	6398.2089	25.5928356	33.17967
3LETTER	250	6317.7072	25.2708288	31.65629
4LETTER	250	5843.283	23.373132	20.95185
5LETTER	250	6669.8259	26.6793036	34.07703
6LETTER	250	6251.7759	25.0071036	28.71788

ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	1430.288	4	357.5719901	12.03276	1.34E-09	3.734311
Within Groups	36997.1	1245	29.71654581			
Total	38427.387	1249				

SUMMARY - MSE

Groups	Count	Sum	Average	Variance
2 LETTER	250	84779.56	339.1182	121943.7
3LETTER	250	88566.65	354.2666	124828
4LETTER	250	115116.2	460.4647	151901.3
5LETTER	250	68948.51	275.794	95496.23
6LETTER	250	90414.96	361.6598	123238.7

ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	4410090	4	1102523	8.928638	4.15E-07	3.734311
Within Groups	1.54E+08	1245	123481.6			
Total	1.58E+08	1249				

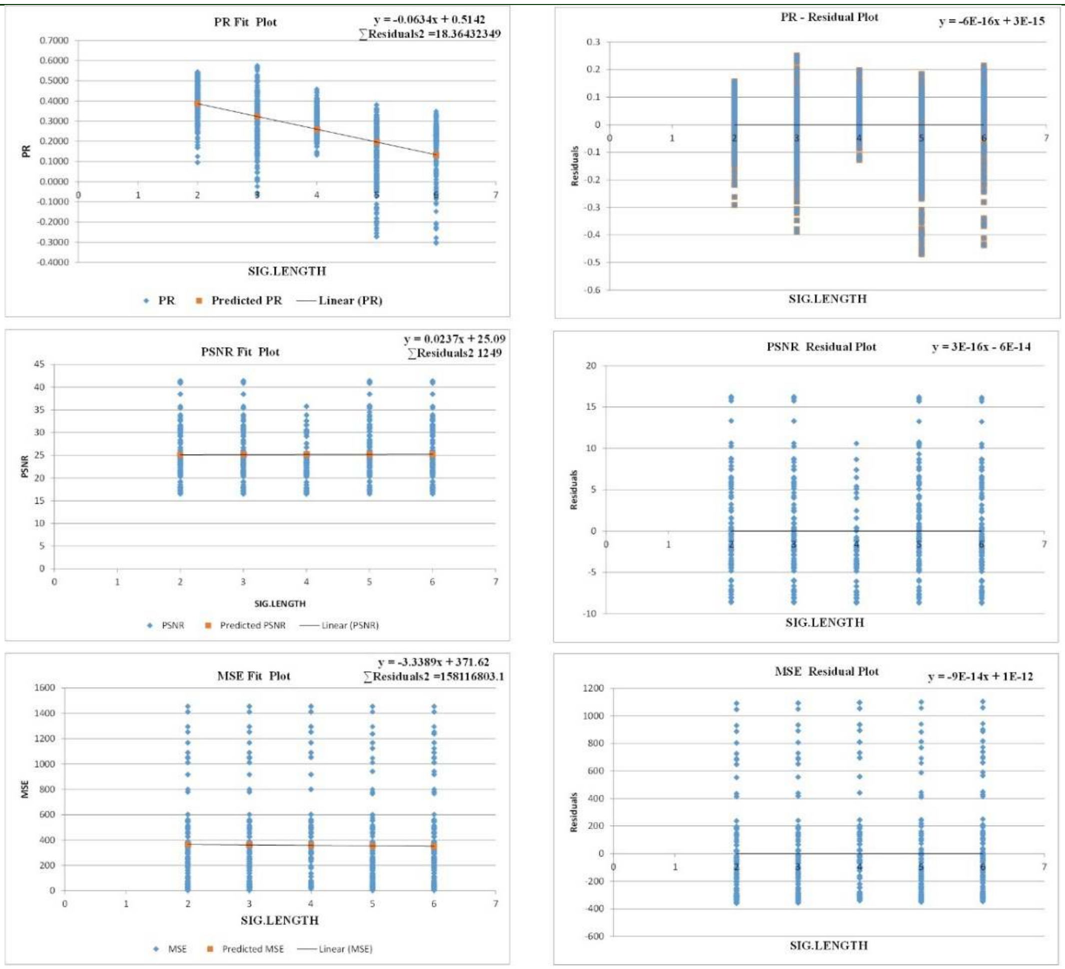


Figure 10. Residual based Linearity Comparison Study

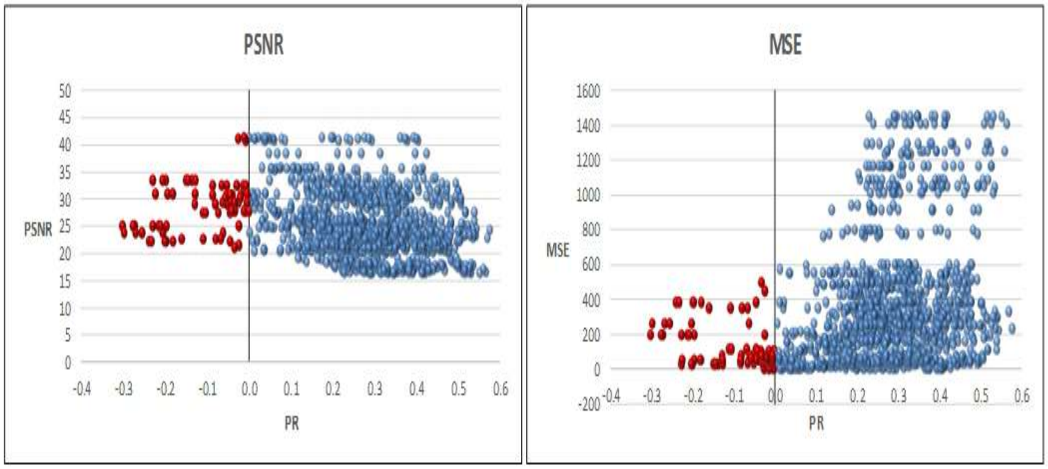


Figure 11. PR as an Efficient Requirement Controlling Parameter