Anamorphic Image Steganography – Enhancing Data Security through Visual Distortion

[1] ABSTRACT:

A large amount of data is shared during communication in the digital age. To ensure the prevention of any unauthorized access and manipulation of this data, one of the most widely used measures of safety is steganography. Steganography is the process of concealing textual data within images without affecting the quality of the image. Traditional steganography methods have proven to be quite effective in maintaining the security of the data. This research, however, aims to add another layer of security to traditional steganography with the use of anamorphic images instead of regular images. Anamorphic images are distorted images that appear regular only when viewed from a particular viewpoint. These images are generated by transforming the original image into a new, larger image, thereby resulting in the formation of gaps between successive pixel positions. The amount of distortion created after transformation varies on the viewing angle, height and distance between the viewer and the original image. Our research aims to implement steganography in anamorphic images by embedding the text within the distorted regions of the images. These regions can be calculated only using equivalent values of the viewing angle, height and distance taken during the transformation which provides an additional layer of security to the data. This research also derives the maximum length of data that can be embedded within an anamorphic image. Additionally, we transform the distorted image back to the original image and compare the original image with the restored image using metrics such as Structural Similarity Index (SSIM), Peak Signal-to-Noise Ratio (PSNR), and Mean Squared Error (MSE).

[2] INTRODUCTION:

[2.1] Anamorphosis

[2.1.1] History of Anamorphosis

Anamorphosis is a visual technique or an art that is an altered representation of a particular image such that the image should be viewed from a specific reference point to be identified. [1]

The history of anamorphic images goes back to the 15th-16th century during the Renaissance period when painters, architects and artists like Leonardo Da Vinci explored the idea of distorted images that could be viewed only from a specific viewpoint. One of the most famous pieces of evidence from the 17th century is the German painter Hans Holbein the Younger's painting of a distorted skull entitled "The Ambassadors". It was also during this century that the term "Anamorphosis" was coined from the Greek word meaning "to transform". In the 18th century, anamorphic images were used for the transmission of secret messages related to religion and politics. The 19th century witnessed the work of an anonymous Dutch Author which explores the idea of planar anamorphosis through a diagrammatic representation of a castle. [2]

With the advancement of science and technology in the later 19th – 20th century, scientists began experimenting with anamorphosis in the fields of cinema and photography to create special effects. [3]

[2.1.2] Generation of Anamorphic Images

[4] An anamorphic image is a distorted version of a regular image which appears normal only when viewed from a particular viewpoint. This distortion of the image is achieved through a mathematical transformation of the original image such that the transformed image appears to be in a trapezoidal shape and is a stretched version of the original image as shown in Fig. 1.

Before the transformation, the original image is converted into a greyscale image as the process is more complex when the color channels of a color image are involved. On conversion into greyscale, the image now only has intensity values ranging between 0-255. In addition to this conversion, values of the viewing angle, the height and distance between the viewer and the original image are set. These values are required for the mathematical transformation of the original image into the anamorphic image.

Owing to the stretching of the original image during the transformation, the generated anamorphic image contains gaps between the pixel values of the original image. For the image to appear normal, these gaps are filled with approximate intensity values using Interpolation techniques like Linear Interpolation, Nearest Neighbour and Sample and Hold interpolation. As a result, the original image is now transformed into a trapezoidal shaped image which is our generated anamorphic image.

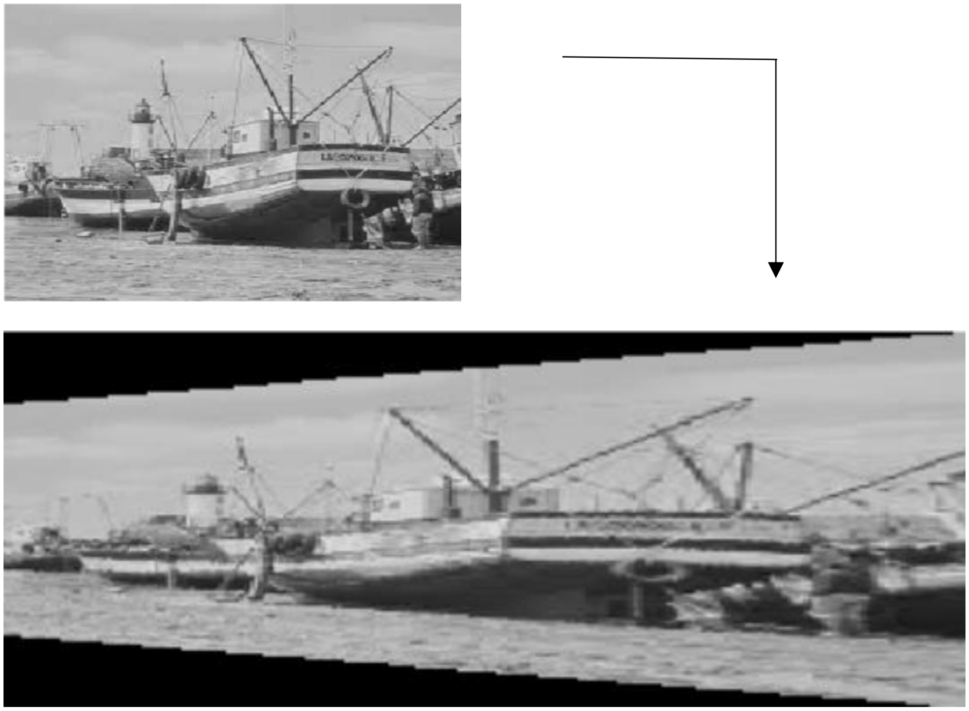


Figure 1: Generation of Anamorphic Images

[2.1.3] Applications of Anamorphosis:

1) Data Security: Anamorphic images are widely used to hide details and messages to protect sensitive data. [4]

2) AR and VR: Anamorphic images are widely used in the gaming industry to provide the users with an immersive experience such as, two marker based mobile augmented reality application to demonstrate 3D anamorphic illusion.[5]

3) Architectural impact: Anamorphosis has an architectural impact in the modern world as it influences how the building is perceived from all sorts of viewpoints. [6]

Although this method finds its roots in an art form, Anamorphosis has evolved in modern technology, majorly in the field of digital image processing. In this paper we are majorly focusing on enhancing the security of the anamorphic image by applying a data hiding technique called ‘Steganography’.

[2.2] Steganography:

Steganography essentially means hiding information within a digital medium and securing our data from potential threats [7]. Steganography majorly aims at concealing the secret message underneath the readable/visual data. [8]. Steganography has set its foot in the digital media and has surpassed all the possible techniques of data hiding [9]

It not only focuses on secure communication but also can help in verifying the authenticity of the data. [10].

[2.2.1] Techniques to implement steganography

1. LSB insertion – This is most extensively used technique; in this method the least significant bit of the pixel values is altered to hide a message [11]
2. Masking and filtering- For images with high contrast Masking and filtering technique is used. This technique essentially manipulates the pixel intensity to hide the secret message.
3. Transform domain techniques – In this technique, raw data is not altered rather the secret message is hidden into the transformed image. The two major ways are by using direct wavelet transform (DWT) and direct cosine transform (DCT). [12]
4. Spread spectrum – This technique is widely used for audio steganography wherein the message is embedded over the wide range of spectrum, making it sturdy enough to be disturbed with any kind of distortion or noise. [13], [14]
5. Substitution technique – This technique is very similar to the LSB method however, in this method we do not change the least significant bit of the pixel value, we change the pixel value and embed our message in it such that it is not evidently perceptible by a human eye.

[2.2.2] Image Steganography:

This type of steganography requires the user to hide the secret message underneath the image by altering the pixel values using methods like least significant bit (LSB) insertion. [15] In today's world the majority of the information is shared over images and therefore becomes very vulnerable to potential cyber-attacks. Steganography plays an important role in providing security for the transmission of data over insecure networks. [16]

[2.2.3] Applications of Steganography:

1. **Digital Watermarking:** Sensitive information like copyrights can be embedded in the image file or any media file to keep intact the ownership authenticity. [17]

2. **Authentication and Validation:** Steganography ensures the authenticity of the data by hiding sensitive information. We can see the implementation on the Internet of things using steganography in this paper. [18]

3. **HealthCare Data Security:** Data related to a patient is extremely crucial as it contains sensitive details regarding the patient's health and wellbeing. [19] This paper discusses the sensitivity of patient's medical information and embedding the crucial information using steganography.

4. **Covert Communication:** Leakage of Data is the biggest potential risk while communicating over the network. This risk can be decreased by applying steganography on the media before sharing over the network. [20] This paper uses a steganographic algorithm for covert communication in the Internet of Things.

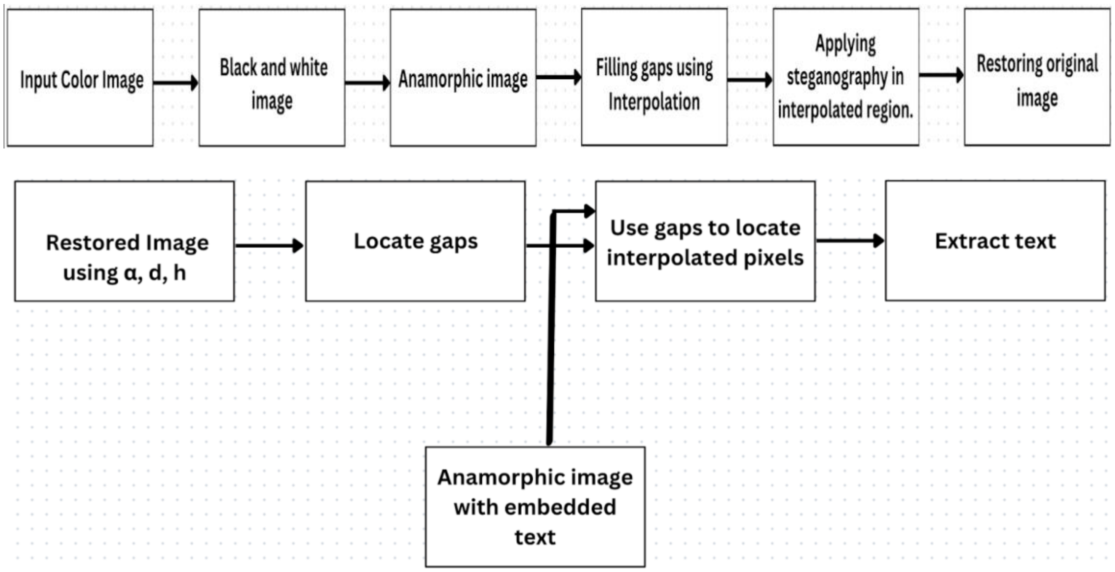

Input Color Image
Black and white image
Anamorphic image
Filling gaps using Interpolation
Applying steganography in interpolated region.
Restoring original image
Restored Image using α, d, h
Locate gaps
Use gaps to locate interpolated pixels
Extract text
Anamorphic image with embedded text

Figure 2: Block Diagram of the Proposed Work

[3] PROPOSED WORK:

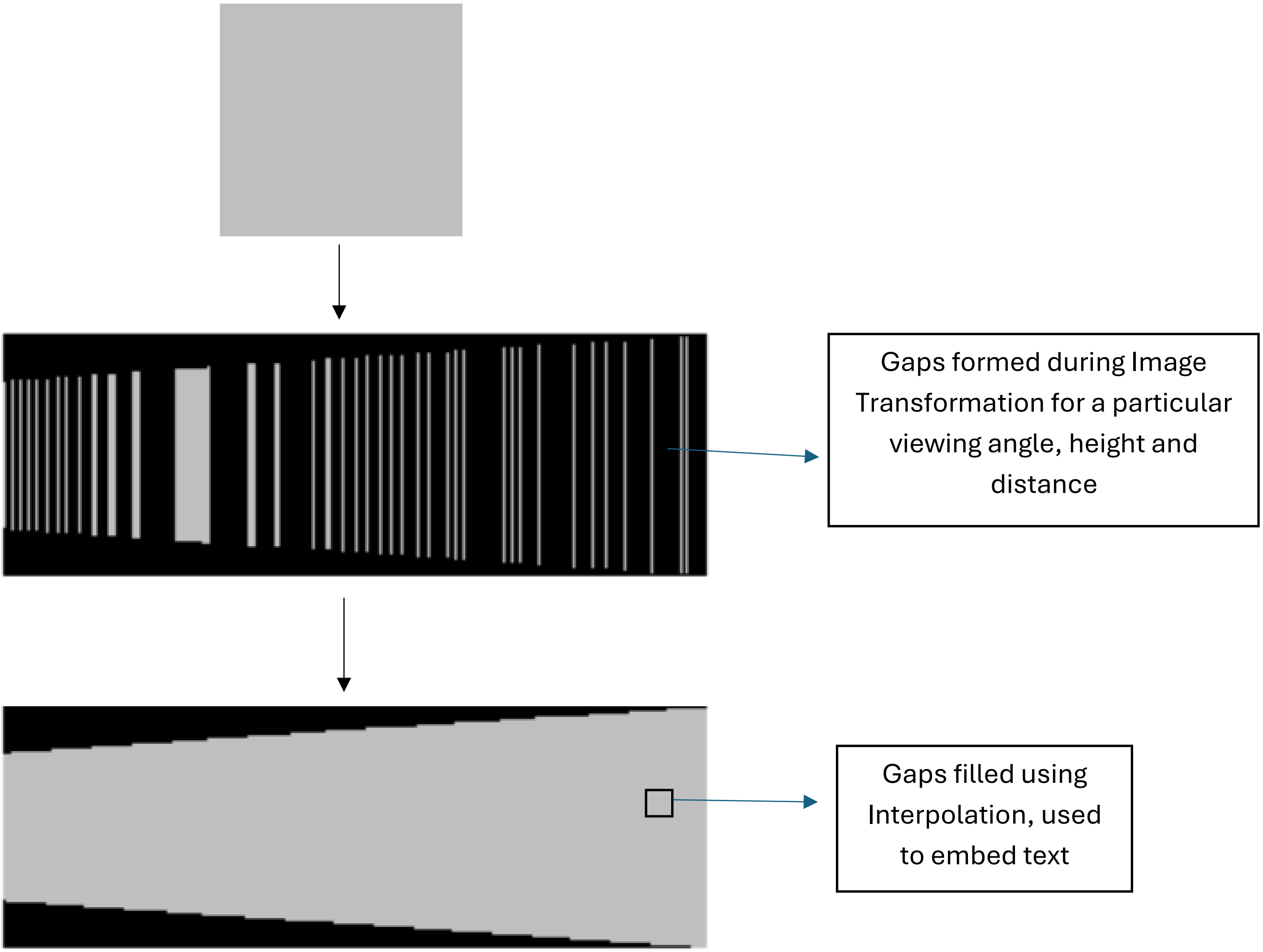
This section illustrates the procedure involved in embedding text in anamorphic images using steganography and discusses the effects associated with the steganographic process during anamorphic transformation. In this work, the generation of anamorphic images, detection of interpolated pixels, and embedding text within these interpolated regions have been systematically analyzed using MATLAB. Steganographic embedding in an anamorphic image refers to the mapping of text data into the new pixel coordinates (x', y') formed during the anamorphic transformation of the original image (x, y). This process increases the complexity of the image matrix and differs from conventional steganography in two key ways: (i) the interpolated gaps generated during anamorphic transformation are non-uniform across the image, while in conventional steganography, pixel locations remain equidistant, and (ii) the anamorphic transformation modifies the geometric shape of the image, converting a rectangular/square matrix into a trapezoidal region (as shown in Fig. 1), whereas conventional steganography typically maintains the original image geometry.

The hidden text is embedded in the gaps introduced during anamorphic transformation, which must be filled using interpolation schemes. The steganographic method is influenced by three parameters that define the anamorphic transformation: viewing angle, distance, and height from the observation point (referred to as the perspective point). Despite the trapezoidal shape of the anamorphic image, a rectangular matrix representation is maintained for computational purposes (as shown in Fig. 1). This matrix is divided into three distinct regions: region 1, containing the valid anamorphic image; and regions 2 and 3, which extend the matrix into a rectangular shape. These additional regions can be filled with either 0 or 255, based on the implementation needs.

The anamorphic transformation maps the original (m × n) matrix into region 1 of a new matrix (M × N), with the interpolated gaps acting as locations for text embedding illustrated in Fig. 3. Regions 2 and 3 are excluded from the embedding process as they contain no valid image data. Assuming the target plane is perpendicular to the line of sight, the coordinates x' and y' of the anamorphic image can be derived from the original coordinates x and y using specific mathematical transformations, where h represents the height from the viewing point, d is the distance from the image, and α is the viewing angle. The maximum length of text that can be embedded depends on the size of the interpolated gaps and the resolution of the anamorphic transformation. Performance metrics are evaluated based on the success of text extraction and image quality post-embedding.

There are multiple approaches to performing steganography; however, in this work, we focus on altering the least significant bit (LSB) of the interpolated pixels. The text to be embedded is first converted into its binary representation, after which each bit is stored in the LSB of an interpolated pixel. The LSB is modified only when the original LSB and the corresponding bit from the text differ, meaning one is 0 while the other is 1. Conversely, if the original LSB and the bit from the text are identical, i.e., both are 0 or both are 1, no changes are made to the LSB. This method of embedding text ensures minimal alteration to the pixel values, thereby preserving the image's quality and fidelity after the steganographic process. By changing only the LSB, we reduce the perceptual distortion in the anamorphic image, ensuring that it closely resembles the original anamorphic image both visually and structurally.

This study further evaluates the performance and quality metrics of the anamorphic images after embedding text, comparing them with the original anamorphic images without hidden data. The impact on image quality is assessed by analyzing various metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE) and Structural Similarity Index Measure (SSIM), ensuring that the embedded text does not significantly degrade the visual quality of the anamorphic image. The observation table (shown in Table 1) presents various images alongside the maximum length of text that could be embedded and the corresponding quality scores of the image after text embedding (as demonstrated by Table 2). This comparison allows for an objective evaluation of the steganographic method's efficiency in maintaining the original image's integrity while successfully hiding the text.



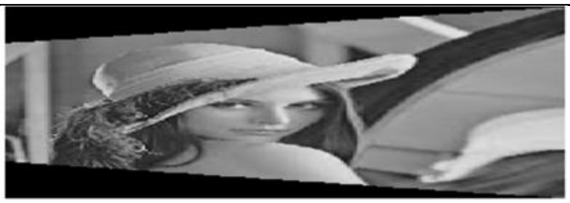
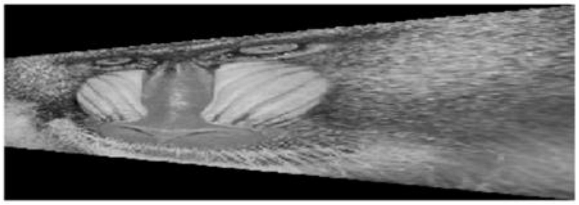
Gaps formed during Image Transformation for a particular viewing angle, height and distance

Gaps filled using Interpolation, used to embed text

Figure 3: Proposed Methodology

[4] RESULT AND DISCUSSION:

The anamorphic transform converts the image into a trapezoidal image. The size of the original image, angle of viewing (α), distance from the viewer (d) and height of the viewing point (h) are all important factors that contribute to the size of the anamorphic image generated. In our work, we have analyzed how different sized images can hide varying number of characters. As discussed earlier, we only hide the text in the interpolated pixels and do not alter the values of pixels which were present in the original image. Thus, the maximum length of text that can be embedded increases with the increase in number of interpolated pixels present in the anamorphic image. Table 1 shows the input image and the anamorphic image generated for various standard test images. The images used are of different sizes and are transformed under the same values of (α, d, h) parameters where α=20, d=1500, h=546. Using the same values of the parameters helps us in identifying the effect of size of the image in finding out the maximum length of message which could be embedded. It is clearly noticeable that an input image of greater size results in a greater capacity for embedding text. This implies that there are a greater number of interpolated pixels in the anamorphic image. Table 1 includes the maximum length of message which could be embedded for each image.

Sl. No.	Input Image (M x N)	Output Image (M' x N')	Maximum length of message which can be hidden
1	 (225 x 225)	 (367 x 1024)	3.3367e+04
2	 (320 x 320)	 (712 x 2083)	1.2131e+05

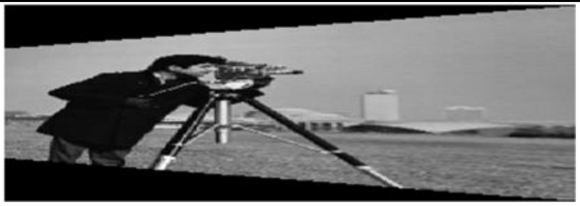
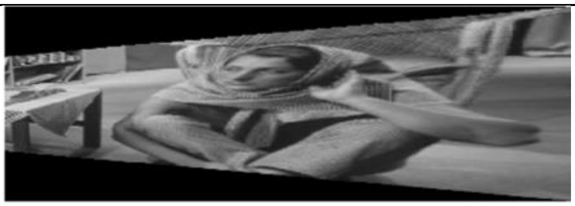
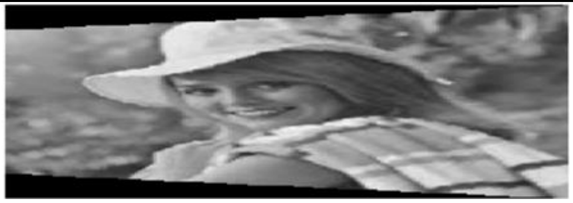
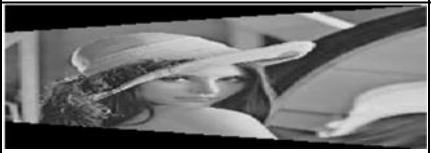
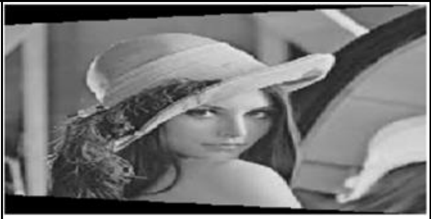
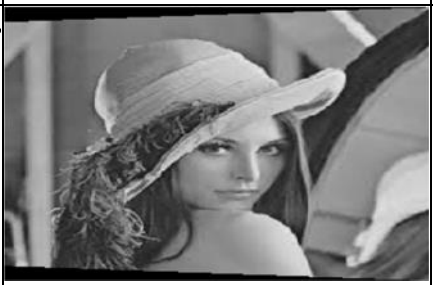
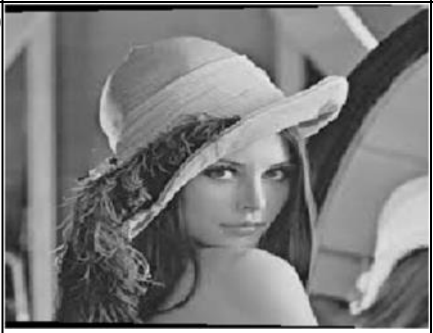
3	(256 x 256)	 (458 x 1338)	5.1371e+04
4	(300 x 300)	 (620 x 1814)	9.2871e+04
5	(150 x 150)	 (202 x 591)	1.0190e+04

Table 1

[5] ANALYSIS:

The original image is transformed into an anamorphic image where we have a limit to how much data we can hide. The amount of data which could be embedded into the anamorphic image depends on the number of interpolated pixels which in turn depend on various parameters. Table 2 is analyzing a standard test image of 225 x 225 under varying values of α, d and h. The results under different parameters vary significantly from one another. Here, we are also comparing the quality of the anamorphic image before and after embedding the text. The text is of fixed length of 82 characters for all the differently generated anamorphic images in the table. We are using three key performance metrics – SSIM (Structural Similarity Index), Mean Squared Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). The SSIM value ranges from -1 to 1 where 1 indicates perfect similarity, -1 indicates perfect anti-correlation and 0 indicates no similarity. The values for our test results show nearly perfect similarity indicating that the anamorphic image is not changing much even after hiding the text. A naked eye will not be able to differentiate between the two images. MSE measures the average squared difference between the anamorphic image before and after hiding text. A lower MSE value indicates less distortion between the two images. Our test results have values close to 0 indicating that the image maintains the original quality. PSNR is a measure of the signal quality of an image after distortion, typically expressed in decibels (dB). A higher PSNR value indicates better image quality, while a lower PSNR indicates greater degradation. Here, we have a significantly higher value for our results justifying better quality for the images.

Sl. No	α	d	h	Anamorphic Image	Maximum length of message which can be hidden	SSIM value	Mean Squared Error (MSE)	Peak Signal-to-Noise Ratio (PSNR)
1	20	1500	546		3.3367e+04	0.999960565	0.000794098	31.001260081 dB
2	30	1750	1010		1.1239e+04	0.999780025	0.002158246	26.658991248 dB
3	40	2000	1678		5.2688e+03	0.999761047	0.003463071	24.605386303 dB
4	50	2500	2979		2.5844e+03	0.999349843	0.004497833	23.469966387 dB

5	60	2750	4763		1.2431e+03	0.998641625	0.005671788	22.462799979 dB

Table 2

The quality of the image after embedding does not only depend on the shape and size of the anamorphic image but also the size of the embedded text. We have already seen the effect of the parameters on the quality. Table 3 shows the impact on the image quality based on the size of the text. We learn that as the size of the text increases, text has to be embedded into a greater number of interpolated pixels resulting in more pixel value changes compared to the original anamorphic image. We have used the same performance metrics to compare the quality difference as Table 2. The results imply that even when large texts are embedded into the image, it does not affect the quality by much. The work done by us gives good results for both small and large texts which cannot be perceived by human eye which makes sure that the hidden text remains safe and secure, and no third person will be able to detect the difference between the two images.

Sl. No	Size of embedded text	SSIM value	Mean Squared Error (MSE)	Peak Signal-to-Noise Ratio (PSNR)
1	100 characters	0.999912228	0.000991988	30.034935882 dB
2	500 characters	0.998979223	0.005102015	22.922582750 dB
3	1000 characters	0.997880168	0.010295364	19.873583029 dB
4	2500 characters	0.992379068	0.025634390	15.911770081 dB
5	5000 characters	0.983240317	0.050923741	12.930796973 dB

Table 3

[6] CONCLUSION AND FUTURE WORK:

Conventional steganography poses various security threats to the embedded text owing to the uniformity in the image pixels in regular images. Anamorphic images, on the other hand, are generated by the stretching of regular images leading to non-uniformity between the image pixels. This distortion can only be achieved through specific values of the viewing angle, height and distance which adds a layer of security to the proposed system. These non-uniform gaps are leveraged in this research as locations to embed text using LSB steganography to ensure minimal change in quality of the image.

The proposed method obtains the maximum number of characters that can be embedded in the anamorphic image. Additionally, the quality of the image is analyzed before and after embedding text using performance metrics like Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE) and Structural Similarity Index (SSIM). The obtained results clearly demonstrate that there is a very minimal change in the image after embedding text of different sizes.

This research can be extended with use of color images in the future. The involvement of color channels while embedding text would provide an additional layer of security to the system. Additionally, LSB steganography poses data manipulation risks due to which other types of steganography can be used and analyzed for improved security. The proposed system can also be made more optimal and computationally less-complex in the future.

[7] REFERENCES:

[1] S. Dubreuil et al., "Artana: Art and Knowledge about Anamorphosis," 2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Christchurch, New Zealand, 2022, pp. 910-911, doi: 10.1109/VRW55335.2022.00306. keywords: {Visualization;Three-dimensional displays;Conferences;Wheels;Teleportation;User interfaces;Spinning;Human-centered computing—Human computer interaction (HCI)—Interaction paradigms—Virtual reality}

[2]https://repozytorium.biblos.pk.edu.pl/redo/resources/28421/file/suwFiles/ZdziarskiA_AnamorphicImages.pdf

[3] M. Ma, H. Shao, J. Zhang, X. Wang and G. Li, "A Calibration Method of Anamorphic Lens Camera Based on Virtual 3D Target," *2019 IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM)*, Hong Kong, China, 2019, pp. 205-210, doi: 10.1109/AIM.2019.8868611.
keywords: {Cameras;Calibration;Lenses;Mathematical model;Three-dimensional displays;Two dimensional displays;Distortion},

[4] L. K. Pavithra, R. Srinivasan, and T. Sree Sharmila. 2022. Optimum anamorphic image generation using image rotation and relative entropy. Multimedia Tools Appl. 81, 27 (Nov 2022), 38971–39001. https://doi.org/10.1007/s11042-022-12982-1

[5] Deborah Rose Buhion, Michaela Nicole Dizon, Thea Ellen Go, Kenneth Neil Oafallas, Patrick Jaspher Joya, Alexandra Cyrielle Mangune, Sean Paulo Nerie, and Neil Patrick Del Gallego. 2023. A Comparative Study of Two Marker-Based Mobile Augmented Reality Applications for Solving 3D Anamorphic Illusion Puzzles. In Proceedings of the 18th ACM SIGGRAPH International Conference on Virtual-Reality Continuum and its Applications in Industry (VRCAI '22). Association for Computing Machinery, New York, NY, USA, Article 3, 1–8. https://doi.org/10.1145/3574131.3574443

[6] Louis Pratt, Andrew Johnston, Nico Pietroni, Bending the light: Next generation anamorphic sculptures, Computers & Graphics, Volume 114, 2023, Pages 210-218, ISSN 0097-8493, Keywords: Anamorphic; Art; Humanities

[7] S. Rahman et al.: Comprehensive Study of Digital Image Steganographic Techniques

[8] R.J.AndersonandF.A.P.Petitcolas,‘‘Onthelimitsofsteganography,’’ IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 474–481, May 1998.

[9] J.*Fridrich,SteganographyinDigitalMedia:Principles,Algorithms,and Applications. Cambridge, U.K.: Cambridge Univ. Press, 2009.*

[10] N. F. Johnson and S. Jajodia, ‘‘Exploring steganography: Seeing the unseen,’’ Computer, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[11] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan and M. Zakarya, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method," in IEEE Access, vol. 10, pp. 124053-124075, 2022, doi: 10.1109/ACCESS.2022.3224745.

keywords: {Steganography;Data privacy;Error analysis;Digital images;Current measurement;Numerical simulation;Robustness;Image steganography;LSB;image quality assessment metrics;histogram analysis;image;capacity;robustness}

[12] A. Sheidaee and L. Farzinvash, "A novel image steganography method based on DCT and LSB," 2017 9th International Conference on Information and Knowledge Technology (IKT), Tehran, Iran, 2017, pp. 116-123, doi: 10.1109/IKT.2017.8258628. keywords: {Discrete cosine transforms;Quantization (signal);Image coding;Frequency-domain analysis;Visualization;Discrete wavelet transforms;steganography;encryption;Discrete Cosine Transform (DCT);least significant bit (LSB);privacy;authentication}

[13] L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," in IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug. 1999, doi: 10.1109/83.777088.

keywords: {Spread spectrum communication;Steganography;Digital images;Signal processing;Authentication;Laboratories;Decoding;Dynamic range;Image restoration;Image coding}

[14] A. A. Krishnan, C. S. Chandran, S. Kamal and M. H. Supriya, "Spread spectrum based encrypted audio steganographic system with improved security," 2017 International Conference on Circuits, Controls, and Communications (CCUBE), Bangalore, India, 2017, pp. 109-114, doi: 10.1109/CCUBE.2017.8394128. keywords: {Spread spectrum communication;Encryption;Ciphers;Signal to noise ratio;Measurement;steganography;spread spectrum;encryption;extraction;cipher}

[15] P. U. Deshmukh and T. M. Pattewar, "A novel approach for edge adaptive steganography on LSB insertion technique," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 2014, pp. 1-5, doi: 10.1109/ICICES.2014.7033807. keywords: {Image edge detection;PSNR;Educational institutions;Visualization;Security;Digital images;Signal processing algorithms;least significant bitbased steganography;stego image;edge adaptive steganography;smooth regions;edge regions}

[16] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan and M. Zakarya, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution

Method," in IEEE Access, vol. 10, pp. 124053-124075, 2022, doi: 10.1109/ACCESS.2022.3224745.

keywords: {Steganography;Data privacy;Error analysis;Digital images;Current measurement;Numerical simulation;Robustness;Image steganography;LSB;image quality assessment metrics;histogram analysis;image;capacity;robustness},

[17] Alvin, A. Wicaksana and M. I. Prasetiyowati, "Digital Watermarking for Color Image Using DHWT and LSB," 2019 5th International Conference on New Media Studies (CONMEDIA), Bali, Indonesia, 2019, pp. 94-99, doi: 10.1109/CONMEDIA46929.2019.8981835. keywords: {Watermarking;Image resolution;Discrete wavelet transforms;Color;Testing;Copyright protection;DHWT;digital watermarking;LSB;steganography},

[18] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan and B. Balusamy, "Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 73-80, Jan. 2020, doi: 10.1109/TSMC.2019.2903785.

keywords: {Internet of Things;Biomedical imaging;Elliptic curves;Public key;Authentication;Confidential data;cryptography;data security;Internet of Things (IoT);steganography;user authentication},

[19] Ramyashree, P. S. Venugopala, S. Raghavendra and B. Ashwini, "CrypticCare: A Strategic Approach to Telemedicine Security Using LSB and DCT Steganography for Enhancing the Patient Data Protection," in IEEE Access, vol. 12, pp. 101166-101183, 2024, doi: 10.1109/ACCESS.2024.3430546.

keywords: {Watermarking;Discrete cosine transforms;Steganography;Security;Robustness;Medical diagnostic imaging;DICOM;Steganography;Signal to noise ratio;Discrete cosine transform;least significant bit;steganography;healthcare;mean squared error;peak signal-to-noise ratio;structural similarity index},

[20] R. Meng, Q. Cui, Z. Zhou, Z. Fu and X. Sun, "A Steganography Algorithm Based on CycleGAN for Covert Communication in the Internet of Things," in IEEE Access, vol. 7, pp. 90574-90584, 2019, doi: 10.1109/ACCESS.2019.2920956.

keywords: {Internet of Things;Generators;Monitoring;Gallium nitride;Generative adversarial networks;Deep learning;Security;Internet of Things (IoT);steganography;CycleGAN;image-to-image translation},