**A Reversible Data Hiding Algorithm for Secured E-Healthcare Applications**

*Submitted in partial fulfillment of the requirements for the degree of*

Bachelor of Technology

in

**Electronics and Communications Engineering**

*by*

|  |  |
| --- | --- |
| **Anasua Choudhury** | **18BEC0694** |
| **Harsh Vardhan Chaudhry** | **18BEC2035** |
| **Arkyajyoti Saha** | **18BEC0938** |

## Under the guidance of

## Prof. Dr. Thanikaiselvan V.

**SENSE**

**VIT, Vellore.**



April, 2022

**DECLARATION**

I hereby declare that the thesis entitled “A Reversible Data Hiding Algorithm For Secured E-Healthacare Applications" submitted by me, for the award of the degree of *Bachelor of Technology in Electronics and Communications Engineering* to VIT is a record of bonafide work carried out by me under the supervision of Prof. Thanikaiselvan V.

I further declare that the work reported in this thesis has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Place: Vellore

Date: 27/04/22

**Signature of the Candidate**

### CERTIFICATE

This is to certify that the thesis entitled “A Reversible Data Hiding Algorithm for secured E-Healthcare Applications” submitted by **Anasua Choudhury 18BEC0694, Harsh Vardhan Chaudhry 18BEC2035 and Arkyajyoti Saha 18BEC0938 & Reg. No**, **Sense** VIT, for the award of the degree of *Bachelor of Technology in Programme*, is a record of bonafide work carried out by him / her under my supervision during the period, 01. 12. 2018 to 30.04.2019, as per the VIT code of academic and research ethics.

The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university. The thesis fulfills the requirements and regulations of the University and in my opinion meets the necessary standards for submission.

Place : Vellore

Date :27/04/22 **Signature of the Guide**

**Internal Examiner External Examiner**

Head of the Department

B.Tech

## ACKNOWLEDGEMENTS

We take this opportunity to express our immense gratitude to our guide, Dr. Thanikaiselvan V, Assisstant Director Department of Communications Engineering, Vellore Institute of Technology, Vellore, for his invaluable guidance, constant encouragement and kind help at various stages for the execution of this project work.

We are grateful to the PhD students who, under the guidance of our guide Dr. Thanikaiselvan V, Department of Communication Engineering, provided valuable assistance and insight during ongoing experimentation.

And last but not the least, we thank all those friends who helped us in the course of this entire project work.

Anasua Choudhury(18BEC0694)

Harsh Vardhan Chaudhry(18BEC2035)

Arkajyoti Saha(18BEC0938)

# Executive Summary

The role of telemedicine in healthcare is growing everyday with thousands of digital operations across the field to make Healthcare efficient, accessible and secure. One such digitalized operation in the domain is the communication of patient information electronically. This comes with the evergreen threat of middle-men and hackers who can steal this information or tamper with it.

With an increase in accessibility of telediagnosis for patients, the emphasis has been brought on the secure communication of patient image or text-based reports to its various remote centers. This makes the access to a secure means of patient data communication essential to the e-healthcare framework. The proposed algorithm employs an Integer Wavelet Transform (IWT) and Elliptic Curve Cryptography (ECC) based asymmetric key hill cipher approach and chaotic maps for encryption of the medical images and a histogram-shift based reversible data hiding for secure transmission of the medical images. The patient data is decomposed using IWT before encryption using the ECC key hill cipher algorithm for first level of encryption and chaotic maps for the second level of encryption. The data transmission is them hidden using histogram-shift based approach before recovery at end point.

In order to measure the efficiency of the proposed algorithm we have employed and verified the values of the entropy, peak to signal noise ratio (PSNR), unified average changing intensity (UACI) against their critical values and the correlation between pixels along horizontal, vertical and diagonal directions is measured.

**CONTENTS Page**

**No.**

**Acknowledgement i**

[Executive Summary](#_TOC_250004)

Table of Contents

[List of Figures7](#_TOC_250003)

[List of Tables](#_TOC_250002)

Abbreviations

[Symbols and Notations](#_TOC_250001)

1. [INTRODUCTION](#_TOC_250000) 
   1. Objective
   2. Motivation 2
   3. Background 3
2. PROJECT DESCRIPTION AND GOALS 3
3. TECHNICAL SPECIFICATION 3
4. **DESIGN APPROACH AND DETAILS (as applicable)** .
   1. Design Approach / Materials & Methods .
   2. Codes and Standards .
   3. Constraints, Alternatives and Tradeoffs .
5. **SCHEDULE, TASKS AND MILESTONES** .
6. **PROJECT DEMONSTRATION** .
7. **COST ANALYSIS / RESULT & DISCUSSION (as applicable)** .

|  |  |  |
| --- | --- | --- |
| 8 | **SUMMARY** | . |
| 9 | **REFERENCES** | . |
|  | **APPENDIX A** | . |

### List of Figures

|  |  |  |  |
| --- | --- | --- | --- |
| **Figure No.** |  | **Title** | **Page No.** |
| 2.1 | Figure caption |  | 13 |
| 2.2 | Figure caption |  | 15 |

(In the chapters, figure caption should come below the figure and table caption should come above the table. Figure and table captions should be of font size 10.)

### List of Tables

**Table No. Title Page No.**

2.1 RSA vs ECC Required Key Length Comparison

2.2 RSA vs ECC Subjective Study

6.1 Histograms of various test images generated by proposed model

6.2 Correlation Coefficient of various test images generated by the proposed model

6.3 Entropy of various test images generated by the proposed model

6.4 NPCR and UACI of various test images generated by the proposed model

6.5 PSNR of various test images generated by the proposed model

## List of Abbreviations

RDH Reversible Data Hiding

RDHEI Reversible Data Hiding for Encrypted Images

VQ Vector Quantisation

PBTL Parametric Binary Tree Labelling

ECC Elliptic Curve Cryptography

IWT Integer Wavelet Transform

MDA Message Digest Algorithm

SHA Secure Hash Algorithm

PKC Public Key Cryptography

RSA Rivest Shamir Adleman

ECDLP Elliptic Curve Discrete Logarithmic Problem

PKI Public Key Infrastructure

MitM Man in the Middle

ML Machine Learning

AI Artificial Intelligence

ANN Artificial Neural Network

API Application Programme Interface

ECCHC Elliptic Curve Cryptography Hill Cipher

PSNR Peak Signal Noise Ratio

SSIM Structural Similarity Index Measure

UACI Unified Average Changing Intensity

NPCR Noise Pixel Changing Rate

APCC Adjacent Pixel Correlation Coefficient

MSE Mean Squared Error

PEE Prediction Error Expansion

## Symbols and Notations

f CFO

nA Private Key of User A

nB Private Key of User B

G Generator Point on the Graph

PA Public Key Of user A

PB Public Key of user B

KI Initial Key 1

K2 Initial Key 2

Km Self Invertible matrix of mXm

∈ Belong to a range

Int Integer

 NCF

**Introduction**

* 1. **Objective**

Past scams and news headlines over the years in the field of medicine have taught us the importance of secure patient data communication in an integrated e-healthcare framework that is an integral part of our digital, data-driven world today. With an increase in internet threats, the need for new and efficient techniques of encryption of data is ever increasing. Discrepancies in data in such scenarios can lead to a faulty diagnosis and fatal consequences and hence emphasizes the need for an algorithm that hides patient information during data communication and retrieves hidden data efficiently. The project objective is to create a strong image encryption and data hiding algorithm against the backdrop of an e-healthcare framework which is one of the most vital parts of our digitalized economy. Telemedicine deals with sensitive personal information of patients that range from reports of a recent diagnosis to reports related to long standing medical history of patients. The current telemedicine operations frequently require transmission of such patient information to its various remote centers for verification of reports, medical investigations and/or further diagnosis of a patient, etc. A secure reversible data hiding algorithm ensures the safety of such systems that traverse unsecure networks and platforms like the internet. We combine Integer Wavelet Transform (IWT), Hill Cipher and Elliptical Curve Cryptography (ECC) for Encryption of the image and a Histogram-shift based Reversible Data Hiding method is employed for hiding the subject data to be transmitted.

* 1. **Motivation**

The integration of vast areas of traditional healthcare practices with telemedicine has led to a surge in digitalization of various operations in the healthcare domain. One such digitalized operation is the storage and sharing of patient information such as personal details of patients and their recent medical treatments, diagnosis and medical history. An ideal telemedicine practice in today’s e-healthcare framework requires the sharing of patient information to its various remote centers for a complete and efficient healthcare service. This is vital especially in cases where the medical history of a patient or data related to a recent diagnosis is required over a distance for a further stage of disease detection and treatment. In today’s scenario a medical discussion among medical professionals regarding a particular medical case is very common and this is just one form of medical investigation that requires the communication of patient information to various locations. Even in the case of a medical case treated locally, the communication of patient data among various specialized centers in the locality such as centers for gastroenterology, cardiology, gynecology, etc. is vital for a complete diagnosis of the patient. These are just a few of the many examples that make a secure and trustworthy patient data communication method absolutely imperative to the e-healthcare framework. And modern-day healthcare setup is no more feasible without realization of the same. The risks of patient data communication are that of the age-old risk to all types of data and all forms of communication – risk of hackers and middle-men. These entities pose a serious threat to patient data communication as this data maybe intercepted, if not secured satisfactorily through available measures, and maybe stolen, manipulated and tampered with. The stakes are higher in regard to the fact that this is sensitive medical data and missing reports or discrepancies may lead to an incomplete and faulty diagnosis which can be extremely dangerous if not life-threatening. Reversible Data Hiding (RDH) Methods have become more and more creative since it was first put to use with numerous projects proposing new algorithms of RDH that have come to be widely used. Our project takes motivation from a number of such algorithms and proposes a new algorithm of its own. This project proposes an Integer Wavelet Transform (IWT), Hill Cipher and Elliptical Curve Cryptography (ECC) based Image Encryption Algorithm and a Histogram-shift based Reversible Data Hiding.

* 1. **Background**

The concepts and topics explored in this project are backed by strong research with numerous papers giving vivid details on the concepts and those that introduce new techniques of image encryption altogether. One such attempt is done by Kai Gao and Ji-Hwei Horng in their paper that proposes another high-capacity reversible data hiding scheme in scrambled pictures. The substance proprietor first partitions the cover picture into blocks. Then, the square stage and the bitwise stream figure processes are applied to scramble the picture. After getting the scrambled picture, the data hider examines the picture blocks and adaptively chooses an ideal square sort marking procedure. In light of the versatile square encoding, the picture is packed to empty the extra room, and the privileged information are encoded and installed into the extra space [1]. Another paper by Nour Kittawi and Ali Al-Haj presents another algorithm that consolidates cryptography and data hiding strategies to conceal data into encoded grayscale pictures in a reversible way. In view of the proposed algorithm, the first cover picture is encoded before a data hiding system is applied to install two watermarks in the scrambled picture [2]. Another method employs a location dependent weighted picture interjection strategy is proposed to work on the visual nature of the inserted picture. Then, the introduced picture is partitioned into covering blocks, which are arranged in a rising request as indicated by their standard deviations; restricted information is specially implanted in the squares with little deviation so that picture quality isn't mutilated excessively. At last, to improve inserting limit however much as could be expected, how much restricted information bits that can be implanted in non-reference pixels is determined adaptively [3]. Another paper proposes versatile reversible data hiding strategy for JPEG pictures containing different two-layered (2D) histograms is proposed by Shaowei Weng, Ye Zhou, Tiancong Zhang where they specially choose more keen histograms for data inserting later 𝐾 histograms are laid out by developing the 𝑘th (𝑘 ∈ {1, 2, …, 𝐾}) histogram utilizing the 𝑘th non-zero rotating current (AC) coefficient of all the quantized discrete cosine change blocks [4]. Another paper uses RRBE strategy where pre-processing is permitted before picture encryption and the pre- processing involves three fundamental stages: registering prediction-errors, obstructing and marking of the errors. By hindering, we deter the requirement for lossless pressure to when a content proprietor isn't enthused. Lossless pressure is utilized in state-of-the-art schemes to further improve payload. We outperform the earlier expressions taking advantage of legitimate indicators, more productive naming technique and impeding of the prediction errors [5]. Completely novel RDH schemes are increasingly being implemented for example a paper proposes an original RDH algorithms in encrypted images which has a high embedding rate without affecting the bit error rate [6]. Vacating room after encryption (VRAE) is another widely used framework of reversible data hiding for encrypted images (RDHEI)[7]. An efficient RDH algorithm in the encrypted domain in an E-healthcare framework is proposed by Rupali Bharadwaj and Anjali Singh, where the algorithm provides a higher embedding rate by the embedding of a single bit of the patient data in a base (2) numeral framework at each and every pixel of cover image without any occurrences of the underflow and the overflow problem [8]. Another paper by Rupali Bharadwaj is one for the secure communication in an E-healthcare framework where a high-capacity dual image RDH algorithm was presented [9]. Pixel difference is another very important and popularly used technique for the embedding of hiding information. In a paper presented by Fuhu Wu , Xu Zhou , Zhili Chen and Baohua Yang they propose a RDH scheme for encrypted images based on pixel prediction and pixel difference[10]. Another such presentation is that of a proposed RDH algorithm for encrypted images (RDHEI) in light of vector quantization (VQ) prediction and parametric binary tree labeling (PBTL). VQ compression is a lossy image compression strategy, the distinction between the first image and the de-pressurized image is little when the length of codebook is adequate. In this manner, VQ can be applied as an instrument for pixel value prediction. In light of VQ forecast, PBTL strategy is applied to mark the embeddable and non-embeddable pixels. Through versatile setting of boundaries, the altered PBTL can give ideal pixel marking procedures also, along these lines, expand the by and large the overall embedding capacity [11]. Another intends to give a far-reaching approach to communicating information safely between brilliant city applications. Reversible information concealing method is broadly used to safeguard restricted data. Pixel esteem requesting (PVO) is a compelling technique of RDH that sorts the pixels of a square in light of their values. The pixel-based PVO (PPVO) technique changes the prescient way in PVO furthermore, accomplishes a high inserting limit. Notwithstanding, in PPVO, the blunders between the anticipated pixel and the ongoing pixel near zero are not used. Chi‑Yao Weng, Hao‑Yu Weng and Cheng‑Ta Huang propose a novel high-limit reversible information concealing technique in light of PVO and middle preservation to advance concealing limit. The middle protecting methodology in each square is utilized to register the anticipated mistake and to decide the perfection of the area. Assuming the square is a smooth region, more anticipated blunders are produced and fall inside the scope of [− 1, 1]. An adjusted different histogram conspire is applied to conceal messages utilizing anticipated mistake moving. Trial results show that the proposed strategy has prevalent concealing limit exhibitions than that of the past PVO-based strategies [12]. In another presentation during the payload conveyance all the encrypted

data is implanted into DCT coefficients with a mutilation minimization plot, and afterward the helper data produced in the past interaction is implanted in the variable length coding grouping with a plan to enhance the record size extension [13]. Another paper was found to explore the Prediction Error Expansion (PEE) based RDH approach [14]. Another paper by Prasenjit Kumar Das, Mr. Pradeep Kumar and Manubolu Sreenivasulu presented a review of various picture cryptographic calculations proposed somewhat recently with some advance techniques. Also, it gives the different viewpoints used to the picture security [15]. Liqaa Saadi Mezher and Ayam Mohsen Abbass utilized encoded Hill Cipher calculation that multiplied the square network of the obvious text with a non-public key and afterward joined it with the Triple Pass Protocol technique used to recurrent the encryption multiple times without depending on an individual key [16]. Rajaa K. Hasoun, Sameerah Faris Khlebus and Huda Kadhim Tayyeh carried out the RSA calculations over the Slope code to expand its security productivity. This strategy depends on the security of the RSA also, Hill Cipher cryptosystems to observe the private unscrambling keys, and in this manner is substantially more secure what's more, impressive than the two strategies applied independently. Likewise secure and dynamic age of the slope figure grid rather than it are proposed to utilize static lattice[17]. In another paper by Aditya Kumar Sahu and Gandharba Swain a RDH based approach is proposed where the principal approach expands the capacity of LSB coordinating with reversibility utilizing dual Images. Though the subsequent methodology uses four indistinguishable cover images for encrypted information implanting utilizing two stages [18].

1. **Project description**

To lengthen our discussion on the project and dive deeper into the individual components that make up our project algorithm, we attempt to dismantle and describe each idea and concept used to meet our project goals. This project aims to design a reversible data hiding method in which the proposed algorithm encrypts the subject image and hides the data for transmission. This image is the then recovered at end point and decrypted to obtain the original message. Here, we discuss the concepts of encryption and various encryption algorithms that are widely used before moving onto Data Hiding concepts.

* 1. **Image Encryption**

Data security has indicated, in retrospect, a very frequently featured and used operation in Image encryption. Encryption of pictures is proven to be a fruitful technique to convey classified data for which endless systems are uncovered. In any case, it keeps drawing in scientists as utilization of images in all means of digital communication has largely expanded.

* + 1. **Cryptography**

**2.1.1.1 Types of Cryptography**

**2.1.1.1.1 Hash Functions**

A fixed-length hash value is processed in light of the plaintext that makes it incomprehensible for either the items or length of the plaintext to be recuperated. Hash algorithms are ordinarily used to give a digital, unique fingerprint of a document's items, frequently used to guarantee that the record has not been adjusted by an interloper or virus. Hash functions are additionally generally utilized by many operating systems to encode passwords. Hash functions, then, give a component to guarantee the integrity of a document.

The more commonly used Hash functions are Message Digest Algorithm (MDA), Secure Hash Algorithm (SHA), Whirlpool, Tiger, etc.

**2.1.1.1.2 Private Key Cryptography**

Secret key cryptography strategies utilize a solitary key for both encryption and unscrambling. The sender utilizes the key to encode the plaintext and sends the ciphertext to the recipient. The beneficiary applies a similar key to decode the message and recuperate the plaintext. Since a solitary key is utilized for the two functions, secret key cryptography is additionally called *symmetric* encryption.

With this type of cryptography, clearly the key should be known to both the sender and the beneficiary; that, as a matter of fact, is the secret. The greatest trouble with this methodology, obviously, is the circulation of the key (erring on that later in the conversation of public key cryptography).

Secret key cryptography schemes are for the most part ordered as being either stream ciphers or block ciphers.

**2.1.1.1.3 Public Key Cryptography**

Public key cryptography has been supposed to be the main new advancement in cryptography in the last 300-400 years. Present day PKC was first portrayed publicly by Stanford University teacher Martin Hellman and graduate understudy Whitfield Diffie in 1976. Their paper portrayed a two-key crypto framework in which two gatherings could take part in a protected correspondence over a non-secure interchanges channel without sharing a secret key.

Conventional PKC utilizes two keys that are numerically related despite the fact that information on one key doesn't permit somebody to decide the other key without any problem. One key is utilized to encode the plaintext and the other key is utilized to unscramble the ciphertext. The significant point here is that it doesn't make any difference which key is applied first, yet that both keys are expected for the cycle to work. Since a couple of keys are required, this approach is likewise called asymmetric cryptography.

In PKC, one of the keys is assigned the public key and might be publicized as generally as the proprietor needs. The other key is assigned the private key and is never uncovered to another party. Sending messages under this scheme is straight-forward. Public key cryptography is additionally called asymmetric encryption. The more commonly used public key algorithms are RSA, ECC, etc.

**Trapdoor Function**

A trapdoor function is a function that is not difficult to register in one direction, yet expected to be hard to figure the other way (seeing as its reverse) without exceptional data, called the "trapdoor". Trapdoor functions are generally utilized in cryptography.

* + 1. **RSA**

RSA (Rivest-Shamir-Adleman) is the most generally taken on asymmetric cryptographic calculation today. It's widely utilized in encoding site information, messages, programming, etc. A critical thing making RSA tick is its straightforwardness. It depends on straightforward numerical standards and can run quicker contrasted with ECC.

The thing about RSA is that it's been found to be quite vulnerable. Scientists could break the encryption of 12,934 keys out of 6.2 million genuine public keys they had examined and gathered. This implies RSA encryption gives under 99.8% security. While this number could sound promising on paper, with the steadily expanding computational power that PCs presently give, it implies that the RSA calculation will probably be broken soon.

* + 1. **Elliptic Curve Cryptography (ECC)**

As the name recommends, ECC is an asymmetric cryptography method in light of uses of the mathematical construction of elliptic curves over finite fields. The algorithm works on the elliptic curve discrete logarithm problem (ECDLP). This cryptography strategy is more difficult to break since there is no known answer for the numerical problem given by the equation delivering the elliptical curve in a graph. Subsequently, just a single way stays for hackers: a brute-power-attack — or an experimentation approach, as such. This intricacy makes ECC safer contrasted with RSA.

As ECC — by structure — is safer contrasted with RSA in light of the fact that it offers ideal security with more limited key lengths. Subsequently, it requires a lesser load for network and computational power, which converts into a superior client experience. To give a few numbers, RSA can answer 450 solicitations each second with a 150-millisecond normal reaction time, while ECC takes just 75 milliseconds to answer similar number of solicitations each second.

* + 1. **RSA vs ECC**

The essential contrast between RSA versus ECC testaments is in the encryption strength. Elliptic Curve Cryptography (ECC) gives a comparable degree of encryption strength as RSA (Rivest-Shamir-Adleman) calculation with a more limited key length. Accordingly, the speed and security presented by an ECC endorsement are higher than an RSA declaration for Public Key Infrastructure (PKI).

**Table 2.1: RSA vs ECC Required Key Length Comparison**

|  |  |  |
| --- | --- | --- |
| Security (in bits) | RSA Key Length Required | ECC Key Length Required |
| 80 | 1024 | 160-223 |
| 112 | 2048 | 224 - 255 |
| 128 | 3072 | 256 - 383 |
| 192 | 7680 | 384 - 511 |
| 256 | 15360 | 512 + |

The two strategies are pervasive and offer protection from man-in-the-middle (MitM) assaults. Nonetheless, RSA has been seen as defenseless against certain attacks, and it's a question of "when" not "if" RSA will ultimately come up short. Numerous specialists accept that RSA will as of now not be being used when 2030 comes around. ECC, then again, is in its development stage, and numerous clients have begun utilizing it.

**Table 2.2: RSA vs ECC Subjective Study**

|  |  |
| --- | --- |
| RSA | ECC |
| A well established and old public key cryptography method | A newer old public key cryptography method when compared to RSA |
| Uses principles of prime factorization method | Uses the mathematical representation of elliptic curves |
| Simpler than ECC and hence runs faster | More complex and takes more time to run |
| RSA requires bigger key lengths to implement encryption | ECC requires much smaller key lengths to perform encryption |
| RSA has revealed many vulnerabilities and at the end of its utility | ECC is in its maturity phase and is expected to be adapted and scaled up in the future |

* 1. **Reversible Data Hiding**

Reversible information stowing away (RDH) calculations deal with concealing information inside images with the end goal that the first image can be completely recuperated upon the extraction of stowed away information. Concealing data in a picture in a way that doesn't influence the first cover picture pixels or cause a permanent distortion subsequent to removing that data is known as reversible data hiding.

* + 1. **Steganography**

Steganography is the procedure of concealing privileged information inside a common, non-mystery, file or message to keep away from identification; the privileged information is then extricated at its objective location. The utilization of steganography can be joined with encryption as an additional a stage for stowing away or safeguarding data.

Steganography can be utilized to disguise practically any sort of digital content, including text, picture, video or sound content; the data to be covered up can be concealed inside practically some other kind of digital content. The content to be hidden through steganography is frequently encoded prior to being integrated into the harmless appearing cover text file or data stream. In the event that not scrambled, the secret text is regularly handled somehow or another to build the trouble of recognizing the mystery content.

* + 1. **Histogram-shift Based Data Hiding**

The histogram-shifting method is a very well-known method among reversible data hiding techniques. To reach its goal of data hiding, this method shifts all pixel values between the peak and zero points and leaves vacant spaces for data hiding. In histogram-based data hiding the number of pixels in the peak point represent the hiding capacity.

* 1. **Chaotic Maps**

Chaos in natural sciences means a deterministic framework that acts eccentric. in mathematics, a chaotic guide is a guide (in particular, a development work) that displays a tumultuous way of n mathematics, a chaotic map is a map (namely, an evolution function) that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time parameter. Discrete maps usually take the form of iterated functions. Chaotic maps often occur in the study of dynamical systems. Of some kind. Guides might be defined by a discrete-time or a ceaseless time boundary. Discrete guides for the most part appear as iterated capacities. Chaos guides frequently happen in the investigation of dynamical frameworks. This term was initially utilized by Li and Yorke in at 1975.Generally, this peculiarity is considered as a piece of dynamical frameworks that change throughout the time. Tumultuous way of behaving is basically recognized in arithmetic by iterated capacities that profits the irregular values in every emphasis. The created arrangement of values by tumultuous capacities (additionally a circle) variates when begun from the different introductory worth. Disarray implies that every double digit (piece) of the code text ought to rely upon a few pieces of the key, darkening the associations between the two. Dissemination actually intends that on the off chance that we change a solitary piece of the plaintext, (measurably) a big part of the pieces in the figure text ought to change, and likewise, in the event that we change the slightest bit of the code text, around one a big part of the plaintext pieces ought to change. Since a piece can have just two states, when they are all reevaluated and changed starting with one apparently arbitrary position then onto the next, a big part of the pieces will have changed state.

1. **Technical Specifications**

MATLAB can be utilized as an instrument for reproducing different electrical organizations yet the new improvements in MATLAB make it an extremely serious apparatus for Artificial Intelligence, Robotics, Image handling, Wireless correspondence, Machine learning, Data investigation, and so forth. However, its generally utilized by circuit branches and mechanical in the designing space to take care of an essential arrangement of issues its application is huge. An apparatus empowers calculation, programming and graphically envisioning the outcomes.

Applications are:

* **Statistics and machine learning (ML)**
  + **This tool stash in MATLAB can be extremely convenient for software engineers.**
  + **Factual techniques, for example, expressive or inferential can be effectively carried out. So is the situation with AI.**
  + **Different models can be utilized to tackle advanced issues. The calculations utilized can likewise be utilized for huge information applications**
* **Curve Fitting**
  + **The bend fitting tool stash assists with investigating the example of event of information.**
  + **After a specific pattern which can be a bend or surface is acquired, its future patterns can be anticipated.**
  + **Further plotting, working out integrals, subsidiaries, addition, and so forth should be possible.**
* **Control systems**
  + **Frameworks nature can be gotten.**
  + **Factors like a shut circle, open-circle, its controllability and discernibleness, bode plot, Nyquist plot, and so on can be gotten.**
  + **Different controlling methods, for example, PD, PI, and PID can be envisioned.**
  + **The investigation should be possible in the time area or recurrence space.**
* **Signal Processing**
  + **Signs and frameworks and advanced signal handling are educated in different design streams.**
  + **Yet, MATLAB gives the open door to appropriate representation of this.**
  + **Different changes like Laplace, Z, and so forth should be possible on some random sign.**
  + **Hypotheses can be approved. The investigation should be possible in the time-space or recurrence area. There are different implicit capacities that can be utilized.**
* **Mapping**
  + **Planning has numerous applications in different areas.**
  + **For instance, in big information, the MapReduce apparatus is very significant and has numerous applications in reality.**
  + **Robbery examination or monetary misrepresentation identification, relapse models, possibility investigation, anticipating strategies in online entertainment, information checking, and so on should be possible by information planning.**
* **Deep learning**
  + **It’s a subclass of AI that can be utilized for discourse acknowledgment, monetary extortion location, and clinical picture investigation.**
  + **Apparatuses like time-series, Artificial Neural Network (ANN), Fuzzy rationale, or a blend of such instruments can be utilized.**
* Financial analysis
  + A business visionary prior to beginning any undertaking needs to do an appropriate review and the monetary investigation to design the game-plan.
  + The instruments required for this are generally accessible in MATLAB.
  + Components like productivity, dissolvability, liquidity, and strength can be distinguished.
  + Business valuation, capital planning, cost of capital, and so forth can be assessed.
* Image processing
  + The most widely recognized application that we notice pretty much consistently are standardized identification scanners, selfies (face magnificence, obscuring the foundation, face discovery), picture upgrades, and so on.
  + The advanced picture handling additionally assumes a seriously significant part in sending information from distant satellites and getting and disentangling it similarly. Calculations to help all such applications are accessible.
* Text analysis
  + Based on the text, sentiment analysis can be done.
  + Google gives millions of search results for any text entered within a few milliseconds.
  + All this is possible because of text analysis. Handwriting comparison in forensics can be done.
  + No limit to the application and just one software that can do this all.
* Electric vehicle designing
  + Utilized for demonstrating electric vehicles and breaking down their presentation with an adjustment of framework inputs.
  + Speed force examination, planning and mimicking of a vehicle, whatnot.

MATLAB is an intuitive framework whose essential information component is an exhibit that does

not need dimensioning. This permits you to tackle numerously specialized registering issues,

particularly those with the framework and vector plans, in a small portion of the time it would

take to compose a program in a non-intuitive intuitive language like C or Fortran.

The name MATLAB represents framework lab. MATLAB was initially

written to give simple admittance to framework programming created by the LINPACK and

EISPACK projects, which together address the cutting edge in programming for grid

calculation.

MATLAB has developed over a time of years with contributions from numerous

clients. In college conditions, it is the standard instructional device for starting and

propelling courses in arithmetic, designing, and science. In industry, MATLAB is the

device of decision for high-efficiency research, advancement, and investigation.

MATLAB features a gathering of purpose-specific game plans called tool stash.

Critical to most clients of MATLAB, device compartments empower you to learn and apply

explicit development. Apparatus compartments are broad aggregations of MATLAB limits (M-records) that loosen up the MATLAB condition to deal with explicit

classes of issues. Domains in which tool compartments are available to integrate banner getting ready,

control structures, brain frameworks, fleecy reasoning, wavelets, reenactment, and

various others.

The MATLAB system consists of five main parts:

1. The MATLAB language:

This is a significant level grid/exhibit language with control stream explanations, capacities, information structures, input/result, and item arranged programming highlights. It permits both "Programming in the little" to quickly make no-nonsense expendable projects, and "Programming in the enormous" to make total huge and complex application programs.

1. The MATLAB working environment:

This is the arrangement of instruments and offices that you work with as the MATLAB client or software engineer. It incorporates offices for dealing with the factors in your work area and bringing in and sending out information. It additionally incorporates apparatuses for creating, making due, troubleshooting, and profiling M-documents, MATLAB's applications.

1. Handle Graphics:

This is the MATLAB graphics system. It includes high-level commands for two-dimensional and three-dimensional data visualization, image processing, animation, and presentation graphics. It also includes low-level commands that allow you to fully customize the appearance of graphics as well as to build complete Graphical User Interfaces on your MATLAB applications.

1. The MATLAB mathematical function library:

This is an immense assortment of computational calculations going from rudimentary capacities like total, sine, cosine, and complex number juggling, to additional modern capacities like network converse, framework Eigenvalues, Bessel capacities, and quick Fourier changes.

1. The MATLAB Application Program Interface (API):

This is a library that permits you to compose C and Fortran programs that associate with MATLAB. It incorporates offices for calling schedules from MATLAB (dynamic connecting), calling MATLAB as a computational motor, and for perusing and composing MAT-records.

1. **Schedule, Tasks and Milestones**

* **January 2022**

Base Papers and methodologies are finalized in contrast to the existing setup that was selected. The “Base Algorithm” was taken to be an image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher

* **February 2022**

The Base Algorithm (Image cryptography) was implemented by performing Encryption and Decryption on the images and the results were formulated

* **Review 1**

The Base Algorithm (Image cryptography) was implemented by performing Encryption and Decryption on the image and the results were formulated

* **March 2022(Full)**

A histogram-Shifting algorithm was added for Reversible data hiding and results were obtained and formulated.

* **Review 2**

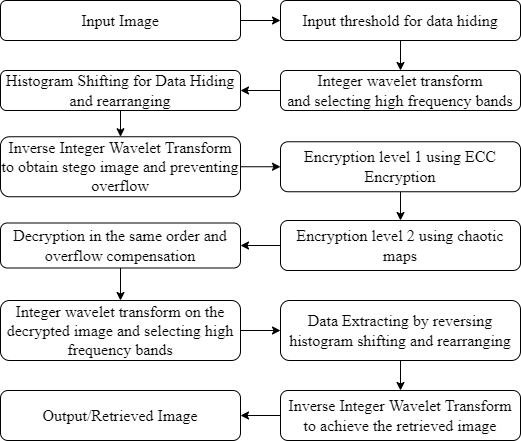
Implementation of the algorithms was performed for reversible data hiding successfully and the results were presented in front of the panel.

* **April 2022**

We added novelty (IWT) Integer Wavelet Transform to our paper and build the report.

1. **Project Design Approach and Demonstration**

**5.1 Project Flowchart**

****

**5.2 Using ECC Multiple Key Hill Cipher**

**5.2.1 Flowchart**

Graphical user interface, text, application, chat or text message

Description automatically generated**Encryption**

**5.2.2 Proposed Cryptosystem**

Suppose the sender (User A) wants to send an image M to the other party (User B) using ECCHC over an insecure channel. Firstly, they should agree on the elliptic curve function E and share the domain parameters {a,b,p,G}, where a,b are the coefficients of the elliptic function, p is a large prime number, and G is the generator point. Then each party needs to choose randomly his private key from the interval [1,p-1]; nA for User A and nB for User B, and generates his public key as follows:

PA=nA.G

PB=nB.G

Each user multiplies his private key by the public key of the other user to get the initial key KI=(x,y)

KI=nA.PB=nB.PA=nA.nB. G=(x,y)

Then computes

K1=x.G=(k11,k12)

K2=y.G=(k21,k22)

The next step is generating the secret key matrix Km by sender and receiver. The inverse of the key matrix does not always exist. So, if the key matrix is not invertible, the recipient cannot decrypt the [ciphertext](https://www.sciencedirect.com/topics/computer-science/ciphertext). To solve this problem, the self-invertible key matrix will be generated, and the same key will be used for encryption and decryption (the matrix K is self-invertible if K=K-1), and no need to find the inverse key matrix. The new approach will be implemented on grayscale images of size 256×256 pixels. The image will be divided into blocks of size four-pixel values. So, each party produces the 4×4 self-invertible key matrix Km by using the proposed method.

Table

Description automatically generated

Let be self-invertible matrix partitioned as

Text

Description automatically generatedText

Description automatically generated with medium confidence The proposed approach assumes that

Then the values of the other partitions of the secret matrix key Km is obtained by solving K12=I-K11, K21=I+K11, and K11+K22=0, where I is the identity matrix.

Now, separate the image pixel values into blocks of size four, each block will be converted to a vector of size 4×1 (P1, P2, P3, …), then multiply the self-invertible key matrix Km by each vector and take modulo 256 to get the ciphered vectors (C1, C2, C3,). After that, reconstruct the ciphered image C from the values in the ciphered vectors and send it to the other party. The following calculations are repeated for each block.

**5.2.3 Approach**

* Key Generation
* User A (The sender)
* Choose the private key nA ∈[1,p-1]
* Compute the public key PA=nA.G
* Compute the initial key KI=nA.PB=(x,y)
* Compute K1=x.G=(k11,k12) and K2=y.G=(k21,k22)
* Generate the self-invertible key matrix Km
* User B (The receiver)
* Choose the private key nB ∈[1,p-1]
* Compute the public key PB=nB.G
* Compute the initial key KI=nB.PA=(x,y)
* Compute K1=x.G=(k11,k12) and K2=y.G=(k21,k22)
* Generate the self-invertible key matrix Km

**5.3 Using Integer Wavelet Transform**

**5.3.1 Flowchart**

Graphical user interface, text, application, chat or text message

Description automatically generated

**5.3.2 Approach**

Text

Description automatically generatedThe extension to two dimensions is immediate as the rows and columns can be treated into a sequence of one-dimensional signals. For the following examples, assume that {cn0}N=1n=0 is the original signal where the superscript indicates level and the subscript indicates a particular point in the signal. Also, {cn1}Ni-1n=0 and {dn1}Mi-1n=0 are its decomposition parts at the first level.

Here

are its low frequency (l) part and high frequency (h) part, respectively. Formulti-levels,

we just treat and repeat the procedure again.



**Diagram

Description automatically generated**Example 1: A (2,2)-wavelet transform by integer calculation. This transformation is similar to a variation of the Haar wavelet transform which uses low and high pass analysis (decomposition) filters given as:

Here, Int () x is an arbitrary rounding function which may have different interpretations. For example, Int () x can be the integer which is nearest to x, or Int( )x may be any integer which satisfies x-1<Int(x)≤ x , etc. It is easy to see that all entries in both {cn1}Ni-1n=0 and {dn1}Mi-1n=0are integers.

**Text, letter

Description automatically generated**Reconstruction

**5.3 Using**

**5.4 Histogram Shifting**

**5.4.1 FLOWCHART**

Graphical user interface, text, application, chat or text message

Description automatically generated

**5.4.2 Approach**

**5.4.2.1. Embedding**

Here we, instead of shifting all the pixels between the peak and minimum point before embedding, we combine the shifting and embedding processes together so that just number of pixels is shifted for a given payload. Therefore, no extra number of pixels will be shifted. The detailed embedding procedure is given below:

* Input: Original 8-bit grayscale image I with MxN pixels and the secret data S
* Output: Stego image Is, the peak point a, the minimum point b, length of secret data |S| and the location map L
* Step 1: Scan the cover image I and constructed its histogram H1(x), x∈[0,255]. In the histogram, obtain the peak point a and the minimum point b. Without loss the generality, we assume a<b
* Step 2: Set k = 0. The variable k is used to indicate the amount of embedded data bits
* Step 3: Scan the cover image I again. If the scanned pixel value is equal to a, a data bit s is extracted from S, set k = k+1 and go to step 4 to embed the data bit s; otherwise, go to step 5
* Step 4: If the data bit s is 1, then the value of scanned pixel is set to a+1; otherwise, no change has to be made for this pixel. Go to step 3 to continue the embedding processes
* Step 5: If the scanned pixel value is within the range (a,b), then the pixel value is add by one. Record the position of pixels whose pixel values is equal to b

**5.4.2.2. Extraction and restoration**

* **Input:**Stego image Is, the peak point a, the minimum point b, the location map L and the length of the secret data |S|
* **Output:** Original 8-bit grayscale image I and the secret data S
* **Step 1:** Set k = 0
* **Step 2:** Scanned the image in the same order as in the embedding phase. If the scanned value is a, let k = k+1 and a bit 0 is extracted. If the scanned value is a+1, let k = a+1 and a bit 1 is extracted. If the scanned value is within the range (a,b) then subtract one from the scanned pixel values. If the position of the scanned pixel is recorded in L, then the value of scanned pixel is set to b
* **Step 3:** Repeat step 2 until k = |S|

The approach has combined both pixel-shifting and data-embedding in a single loop. By doing this, no extra work is required on processing small amount of payload. Therefore, a better quality for stego image and lower computational cost could be achieved.

**5.5 Using Chaotic Maps**

Graphical user interface, text

Description automatically generated**5.5.1 Flowchart**

**5.5.2 Approach**

The chaos-based image cryptosystem architecture generally comprises two phases; the confusion phase and the diffusion phase. The confusion phase is also known as the pixel permutation, in which the pixel positions are rearranged over the whole image while the pixel values remain unchanged, converting the image into an unidentifiable form. Afterward, the diffusion phase is applied, as the former phase is not secure enough and can be easily hacked by an attacker. Hence, when the diffusion phase is executed with the help of a chaotic map, the values of the pixels of the whole image are changed consecutively by the sequence generated from the chaotic systems. Multiple iterations of the confusion–diffusion process are performed until a satisfactory level of security is attained.

**6. Results and discussions**

The proposed cryptosystems all produce the similar results with not much variance. The Encryption side chosen parameters decides the results. There are few parameters to measure the efficiency of the cryptography used. These measures compare between the Original & Encrypted images for knowing the reliability of the cryptosystem implemented. Various methods are applied in this research for the evaluation of the encryption efficiency like Entropy, Peak Signal to Noise Ratio (PSNR), Unified Average Changing Intensity (UACI) and Noise Pixel Changing Ratio (NPCR).

* 1. **Histogram Analysis**

The Histogram of all 10 images is shown below in the table. The histogram of original, encrypted and decrypted images over the interval [0-255] is shown. The encrypted image histogram obtained is uniform showing us the level of security it has obtained. Since the histogram of different images is similar tells us that cryptosystem is working well and making it difficult to crack.

**Table 6.1: Histograms of various test images generated by proposed model**

|  |  |  |  |
| --- | --- | --- | --- |
| Test Image | Stego Image Histogram | Encrypted Image Histogram | Retrieved Image Histogram |
| Lena.jpg |  |  |  |
| Boat.jpg |  |  |  |
| Bridge.jpg |  |  |  |
| Lighthouse.jpg |  |  |  |
| Baboon.bmp |  |  |  |
| Hill.png |  |  |  |
| Einstein.png |  |  |  |
| Cameraman.gif |  |  |  |

* 1. **SCATTER PLOT AND CORRELATION ANALYSIS IN HORIZONTAL, VERTICAL & DIAGONAL DIRECTIONS**

The scatter diagram graphs pairs of numerical data, with one variable on each axis, to look for a relationship between them. If the variables are correlated, the points will fall along a line or curve. The better the correlation, the tighter the points will hug the line.

Adjacent pixels correlation coefficient (APCC), another common measure used in the assessment of the security level for newly designed image encryption algorithms, is based on the well-known fact that, generally in plain-images, any arbitrarily chosen pixel is strongly correlated with its adjacent pixels (either they are diagonally, vertically or horizontally oriented). Consequently, in the case of high-performance image encryption algorithms, adjacent pixels’ correlation scores are expected to be close to zero, i.e., al neighboring pixels considered in the test are weakly correlated. To verify whether the computed APCC is indeed a zero, given the previous study. Have tested if the coefficient follows Student’s 𝑡-distribution, thus confirming that for the encrypted image the adjacent pixels are truly uncorrelated.

For correlations of the adjacent pixels in the plain and cipher image, we randomly choose 1000 pairs of adjacent pixels in horizontal, vertical and diagonal directions from the plain image and its encrypted image. We have also used the following formulas to calculate the correlation coefficient.

Text, letter

Description automatically generated

Where *x* and *y* are the grayscale values of two adjacent pixels in the image, and *S* is the total number of pixels selected from the image. The calculation results are listed in the table below. The figure and table all show that the proposed encryption algorithm can make the adjacent pixels of the encrypted image have extremely low correlation. The plots for all 10 images are obtained and shown below.

**Table 6.2: Correlation Coefficient of various test images generated by the proposed model**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Test Images** | **Correlation Coefficient** | | | | | |
| **Horizontal Direction** | | **Vertical Direction** | | **Diagonal Direction** | |
| **Original Image** | **Encrypted Image** | **Original Image** | **Encrypted Image** | **Original Image** | **Encrypted Image** |
| **Lena.jpg** | 0.9231 | 0.0418 | 0.8997 | 0.0076 | 0.9109 | 0.0014 |
| **Boat.jpg** | 0.8902 | 0.0383 | 0.8379 | 0.0281 | 0.8639 | 0.0143 |
| **Bridge.jpg** | 0.9054 | 0.0101 | 0.8257 | 0.0119 | 0.8301 | 0.0136 |
| **Lighthouse.jpg** | 0.7735 | -0.0072 | 0.6775 | -0.032 | 0.6832 | -0.0014 |
| **Baboon.bmp** | 0.7995 | -0.0154 | 0.7524 | -0.0211 | 0.7240 | -0.0357 |
| **Hill.png** | 0.9222 | 0.0058 | 0.8874 | 0.0085 | 0.8866 | -0.0084 |
| **Einstein.png** | 0.9141 | 0.0032 | 0.8706 | 0.0282 | 0.8891 | -0.0300 |
| **Cameraman.gif** | 0.8971 | -9.5737e-04 | 0.8894 | -0.0262 | 0.8855 | 0.0104 |

* 1. **Entropy**

It measures the randomness of the picture pixel values. Greater the entropy, lesser the probability to find the values. For a plain black image, entropy is 0. For a standard 256x256 image, the ideal and theoretical value of entropy is 8.

****

Where P(x) is the probability of the pixel value x and computed by

P(x) = (the frequency of pixel value x) / (total number of image pixels)

As inferred from the table we can see that the value for all 10 encrypted images is really close to ideal value 8 indicating a good sign.

**Table 6.3: Entropy of various test images generated by the proposed model**

|  |  |
| --- | --- |
| **Test Image** | **Entropy** |
| Lena.jpg | 7.9975 |
| Boat.jpg | 7.9973 |
| Bridge.jpg | 7.9969 |
| Lighthouse.jpg | 7.9967 |
| Baboon.bmp | 7.9970 |
| Hill.png | 7.9970 |
| Einstein.png | 7.9973 |
| Cameraman.giff | 7.9967 |

**6.4 UACI and NPCR**

The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are two most common quantities used to evaluate the strength of image encryption algorithms/ciphers with respect to differential attacks. Conventionally, a high NPCR/UACI score is usually interpreted as a high resistance to differential attacks.

W x H = m\*n

**Text

Description automatically generated**

**Diagram

Description automatically generated with low confidence**

NPCR checks whether all the pixels have been changed. Its value lies in the range [0, 1]. From the table NPCR values, we can say that the values are closer to ideal value 1 indicating higher efficiency of algorithm.

UACI is concerned with average differences between two ciphered images. For a 256x256 image, UACI near to 30 is ideal. From the Table 10, the UACI values are closer to 30 indicating rigidness of the proposed algorithm.

**Table 6.5: NPCR and UACI of various test images generated by the proposed model**

|  |  |  |
| --- | --- | --- |
| **Test Image** | **NPCR (%)** | **UACI (%)** |
| Lena.jpg | 99.62 | 30.5657 |
| Boat.jpg | 99.63 | 28.3217 |
| Bridge.jpg | 99.63 | 29.9265 |
| Lighthouse.jpg | 99.62 | 29.9665 |
| Baboon.bmp | 99.62 | 31.9283 |
| Hill.png | 99.63 | 29.3672 |
| Einstein.png | 99.62 | 28.8745 |
| Cameraman.gif | 99.62 | 35.1664 |

* 1. **PSNR**

The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation.  Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale.

Logo, company name

Description automatically generatedFor the following implementation, let us assume we are dealing with a standard 2D array of data or matrix.  The dimensions of the correct image matrix and the dimensions of the degraded image matrix must be identical.  
The mathematical representation of the PSNR is as follows:

Where

the MSE (*Mean Squared Error*) is:

A picture containing text

Description automatically generated

**f** represents the matrix data of our original image  
**g** represents the matrix data of our encrypted image  
**m** represents the numbers of rows of pixels of the images and I represents the index of that row  
**n** represents the number of columns of pixels of the image and j represents the index of that column  
**MAXf** is the maximum value that exists in our original image.

When comparing the original image with the encrypted image; if MSE increases, then PSNR decreases, and this indicates that the encrypted image is more randomness. The PSNR value for encrypted & decrypted is ∞, which indicates the ideal nature of the proposed cryptosystem.

**Table 6.6: PSNR of various test images generated by the proposed model**

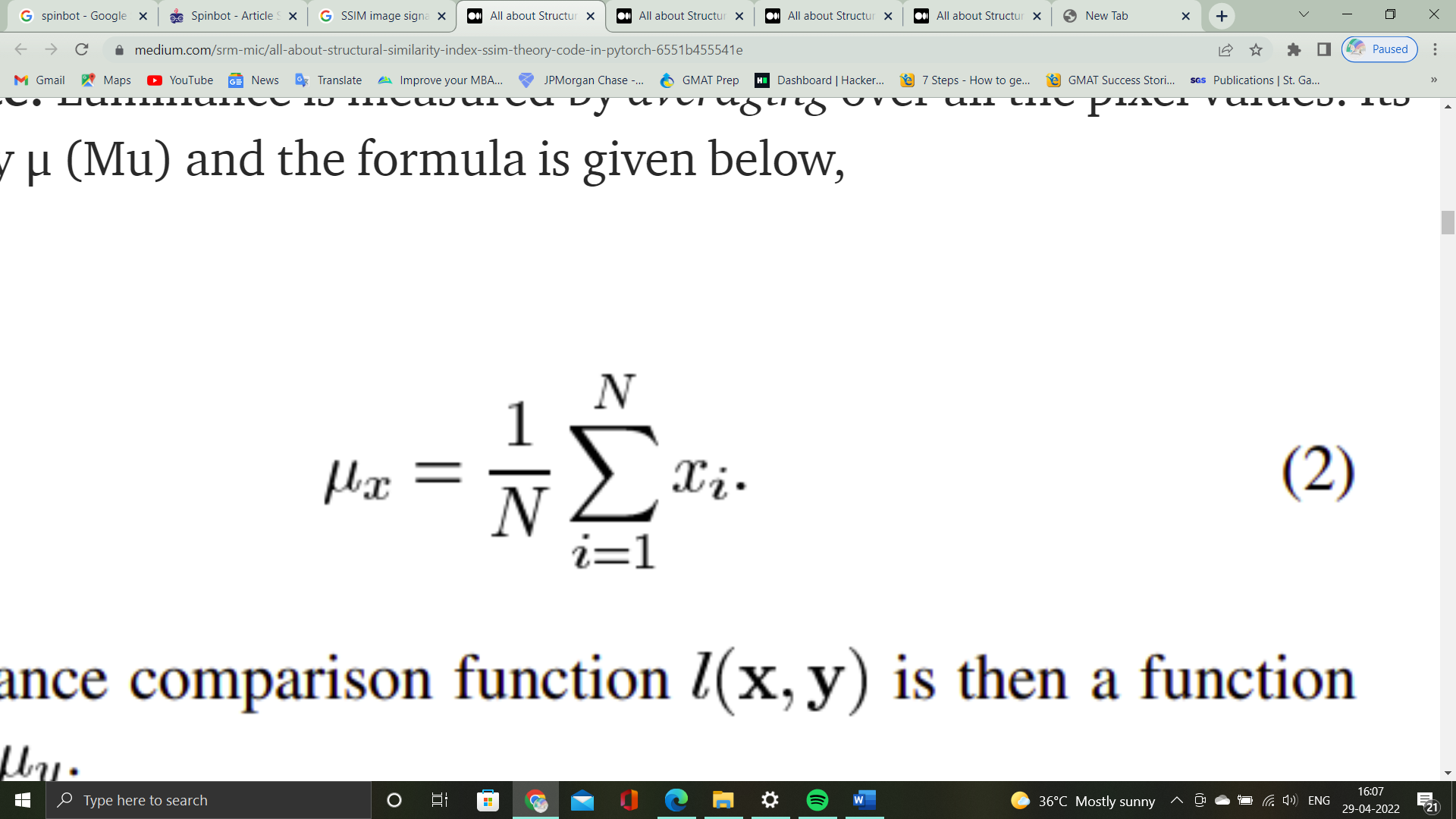
|  |  |
| --- | --- |
| **Test Image** | **PSNR** |
| Lena.jpg | 8.5579 |
| Boat.jpg | 9.3076 |
| Bridge.jpg | 8.7770 |
| Lighthouse.jpg | 8.7524 |
| Baboon.bmp | 8.1541 |
| Hill.png | 8.9756 |
| Einstein.png | 9.1440 |
| Cameraman.giff | 7.3391 |

**6.6 SSIM**

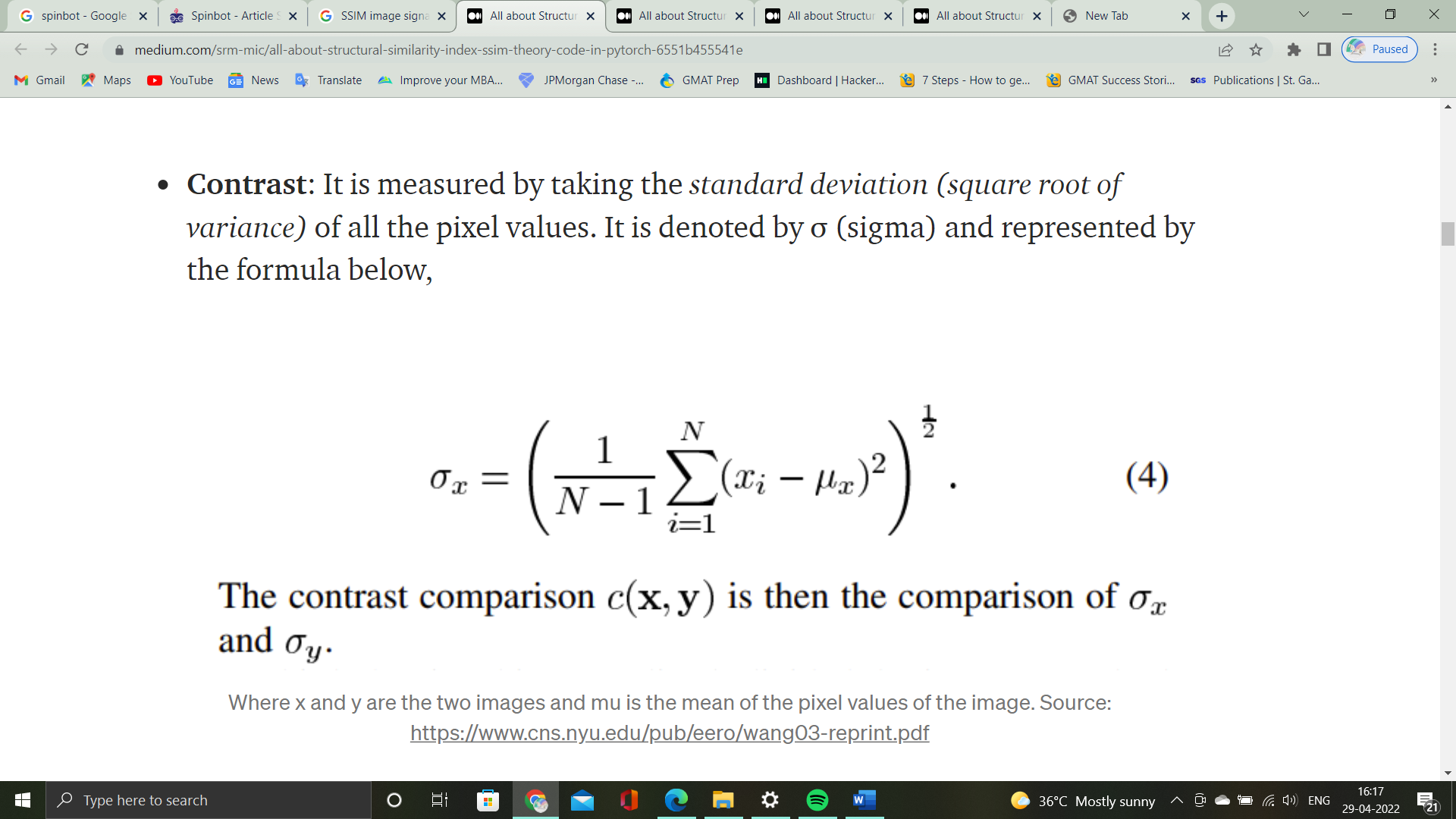
The structural similarity index measure (SSIM) is a method for predicting the quality of various kinds of digital images as well as videos. SSIM is used to measure the similarity of two images. The image quality that is measured is done based on a un-compressed or distortion-free image that is taken as the reference. Hence, it is a full reference metric that requires no less than two images from the very same image capture— a reference image and a processed image.

SSIM metric extract three key features from an image:

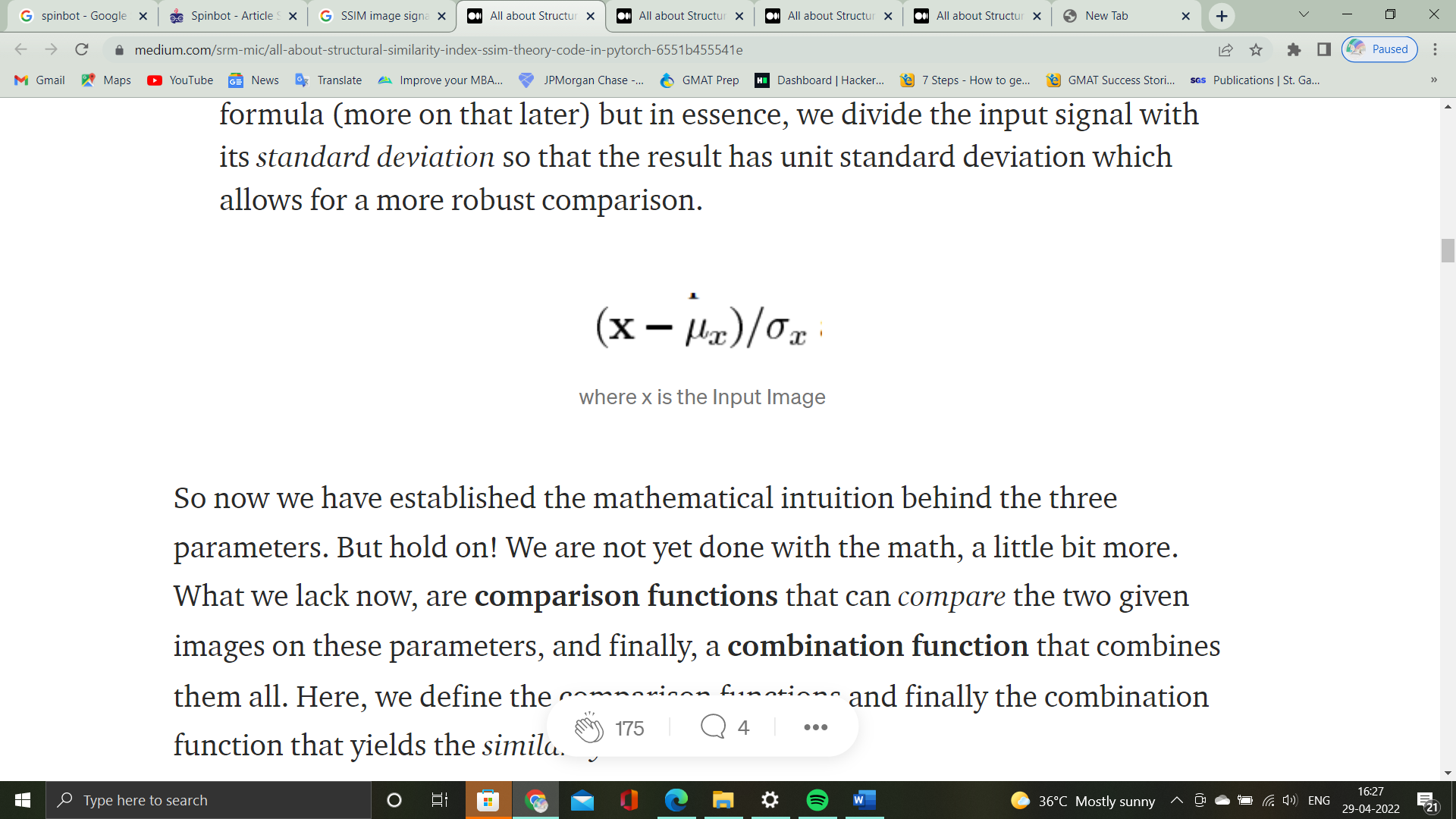
**Luminance**: This is measured by taking the average over all pixel values. This is denoted by μ (Mu) as per the formula given below,



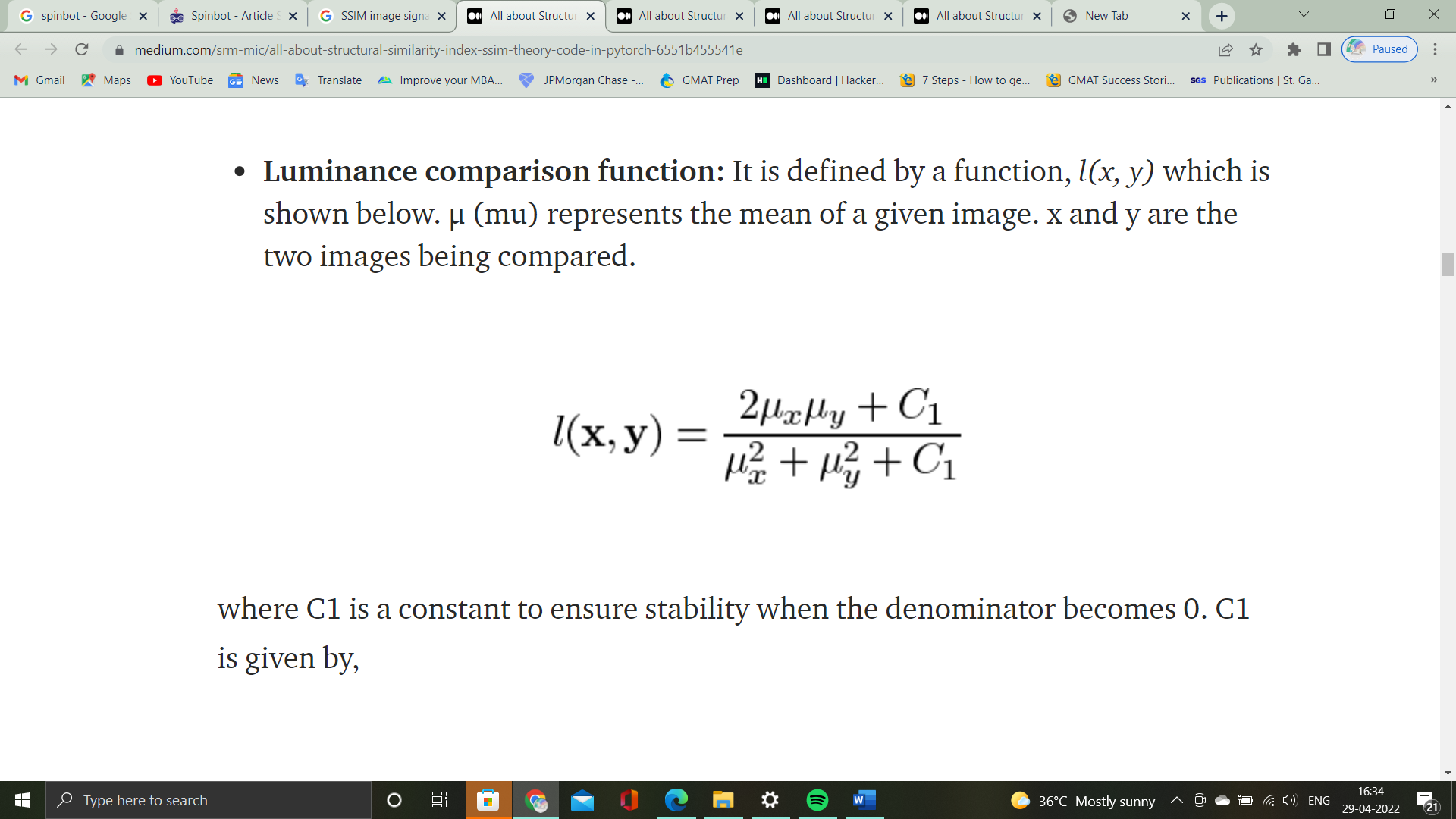
**Contrast**: To measure the standard deviation (square root of variance) of all the pixel values is taken. Its denoted by σ (sigma) as per the formula below,



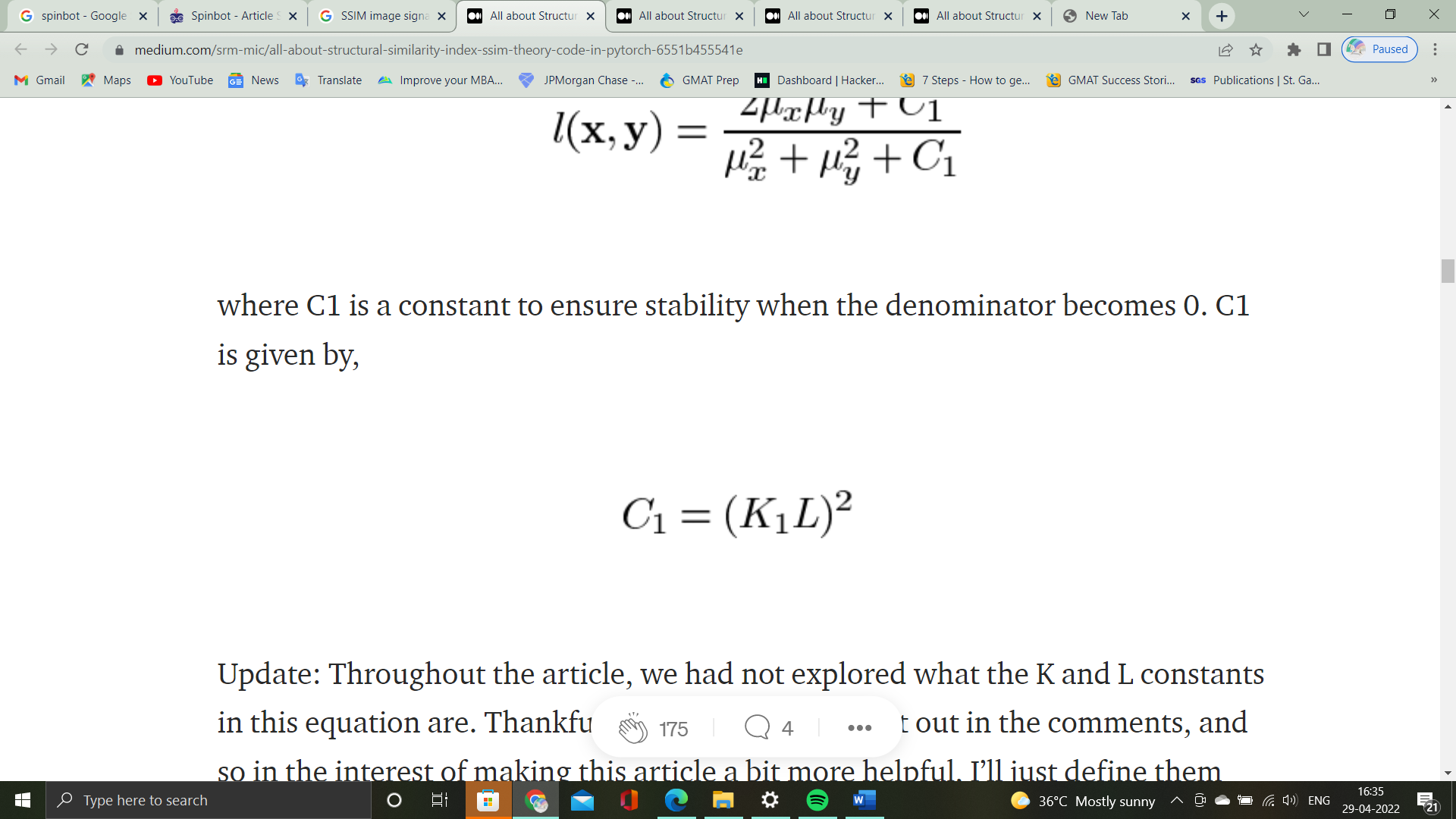
**Structure:**  The structural comparison, in actuality is done by putting to use a consolidated formula. However, in essence, we divide the input signal with the standard deviation of the signal. This is done so that the result has a unit standard deviation which allows for a more robust comparison.

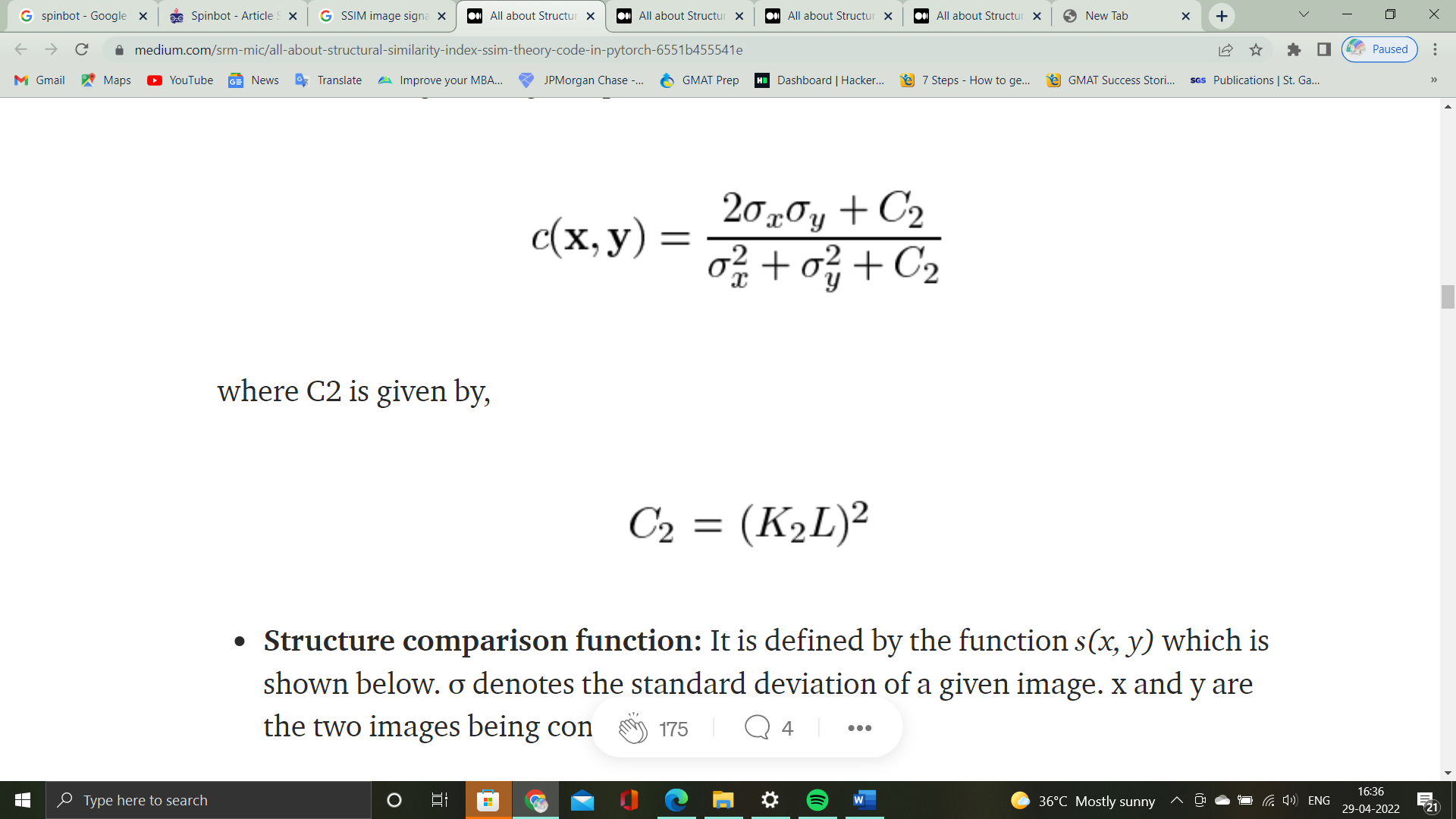
here, x is the input

And the combination functions are given as follows for **Luminance comparison, Contrast comparison, Structure comparison respectively.**

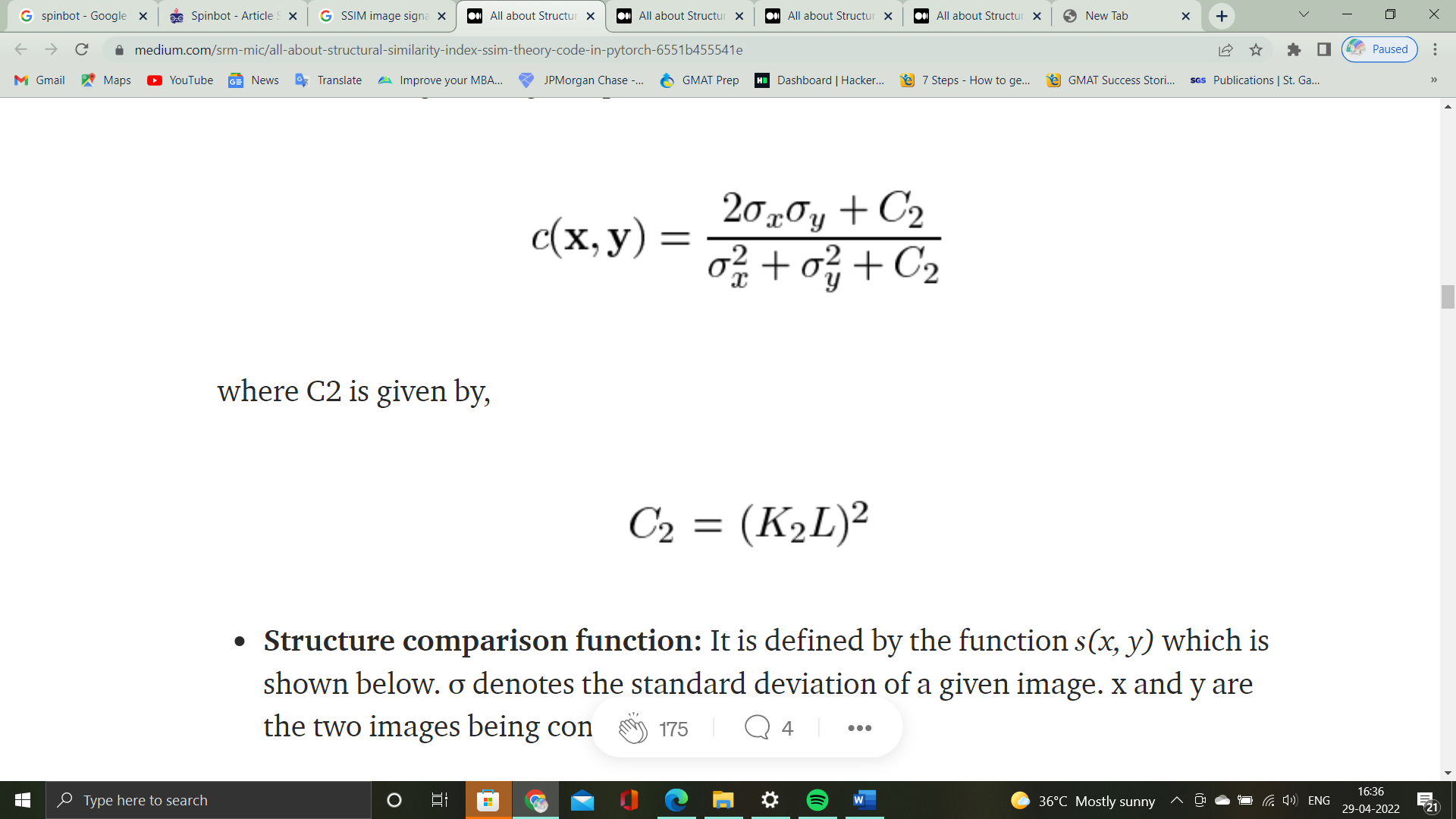


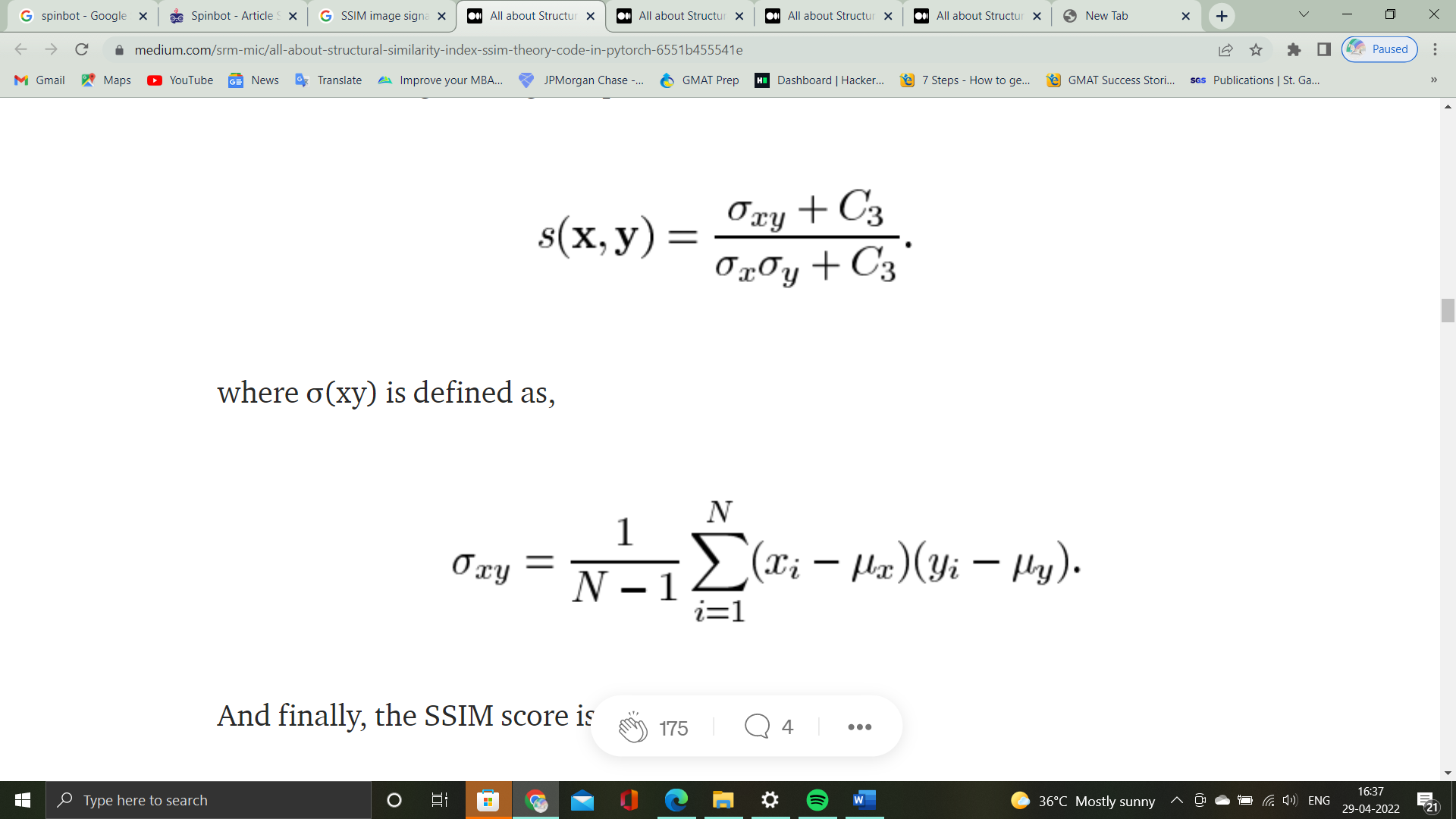
Here, the constant C1 is given by,



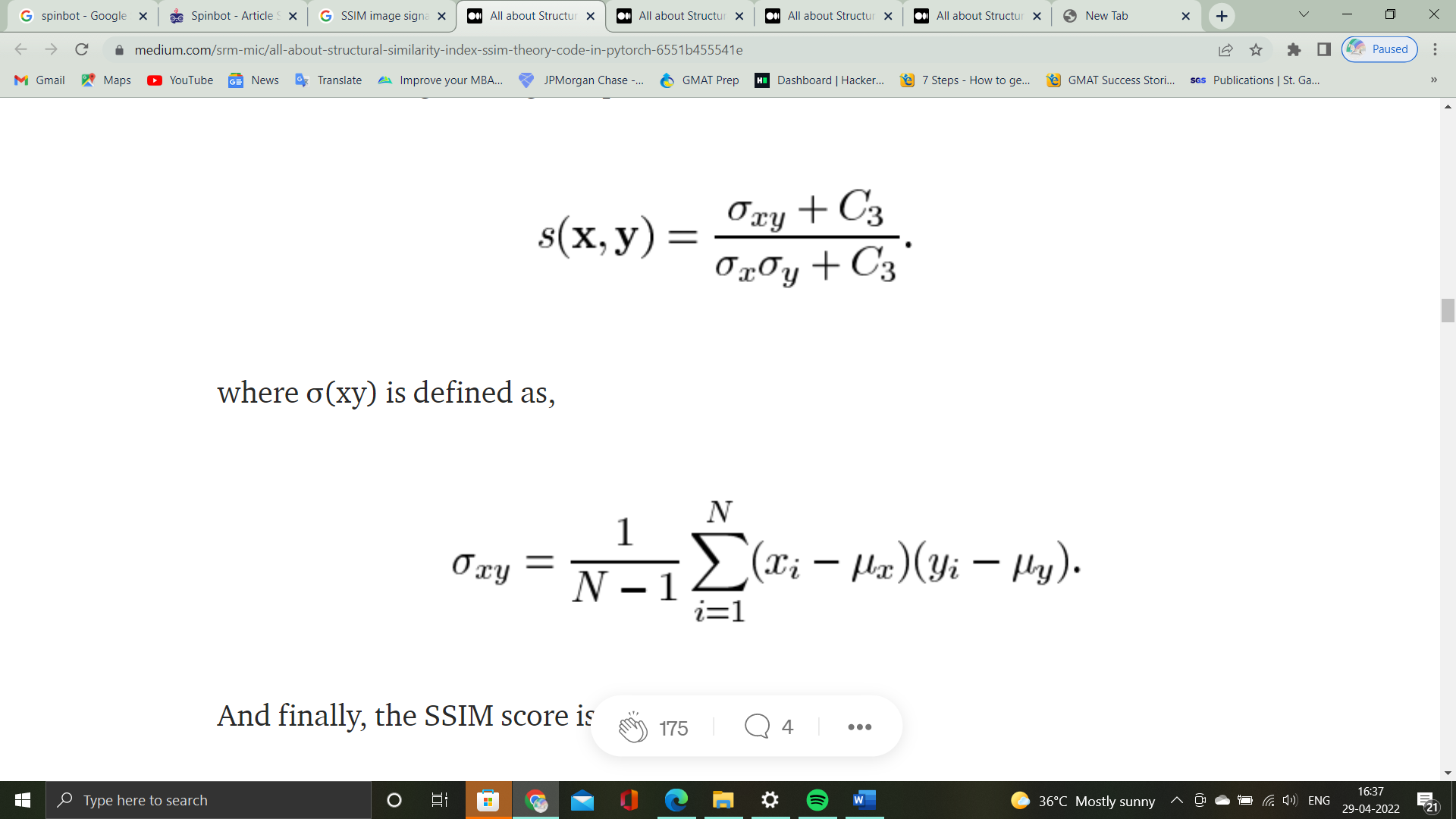


Here, the constant C2 is given by,

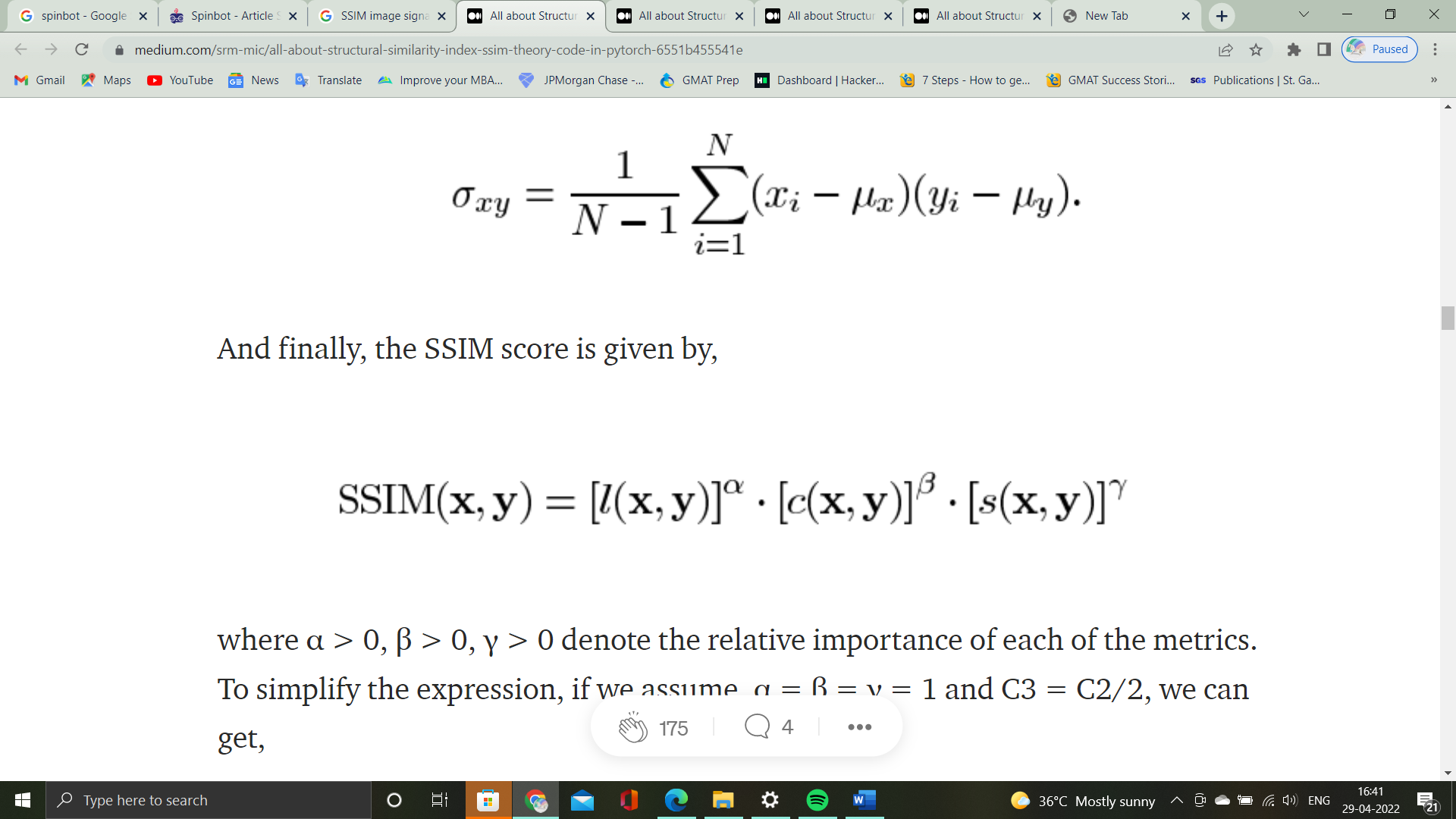




Where,



Finally, the SSIM score is given by the combination function,



**7. Cost Analysis**

The Project that we did is simulation based so all we need is a licensed MATLAB Software and a computer with high end configuration so that the simulation time would be more efficient. The project can be implemented free of cost if the tools mentioned are readily available.

**7. Summary**

This report demonstrates in vital detail our final project that was completed over the course of our final semester under the able guidance of our project guide. This report documents a new image encryption technique complete with the proposed algorithm, project demonstration and performance analysis measured against the critical values and ideal characteristics. Our proposed model employs an Integer Wavelet Transform based approach to the widely used methods of ECC and Hill Cipher before finally employing a Histogram-shift based data hiding technique as a means to hide the information. The same has been measured and verified against performance measures such as entropy, NPCR, UACI and Correlation coefficient of the pixels in different directions for various cases. This was performed on 10 such images and the results were recorded and compared with each other and the various parameters as mentioned. We concluded a satisfactory and reliable RDH algorithm that can be put to use on medical images for ensured security during transmission.

**10. References**

1. [1-s2.0-S1047320322000372-main.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\1-s2.0-S1047320322000372-main.pdf)
2. [Kittawi-Al-Haj2022\_Article\_ReversibleDataHidingUsingBitFl.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\Kittawi-Al-Haj2022_Article_ReversibleDataHidingUsingBitFl.pdf)
3. [1-s2.0-S0165168422000056-main.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\1-s2.0-S0165168422000056-main.pdf)
4. [1-s2.0-S1047320322000414-main.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\1-s2.0-S1047320322000414-main.pdf)
5. [1-s2.0-S1047320322000347-main.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\1-s2.0-S1047320322000347-main.pdf)
6. [1-s2.0-S0923596522000388-main.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\1-s2.0-S0923596522000388-main.pdf)
7. [Reversible data hiding with adaptive difference recovery for.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\Reversible%20data%20hiding%20with%20adaptive%20difference%20recovery%20for.pdf)
8. [Bhardwaj-Singh2021\_Article\_AnEfficientReversibleAndSecure.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\Bhardwaj-Singh2021_Article_AnEfficientReversibleAndSecure.pdf)
9. [Hiding-patient-information-in-medical-images--an-encrypted-dual-image-reversible-and-secure-patient-data-hiding-algorithm-for-EhealthcareMultimedia-Tools-and-Applications.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\Hiding-patient-information-in-medical-images--an-encrypted-dual-image-reversible-and-secure-patient-data-hiding-algorithm-for-EhealthcareMultimedia-Tools-and-Applications.pdf)
10. [A reversible data hiding scheme for encrypted images with pixel.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\A%20reversible%20data%20hiding%20scheme%20for%20encrypted%20images%20with%20pixel.pdf)
11. [Reversible\_Data\_Hiding\_Scheme\_Based\_on\_VQ\_Prediction\_and\_Adaptive\_Parametric\_Binary\_Tree\_Labeling\_for\_Encrypted\_Images.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\Reversible_Data_Hiding_Scheme_Based_on_VQ_Prediction_and_Adaptive_Parametric_Binary_Tree_Labeling_for_Encrypted_Images.pdf)
12. [Weng2022\_Article\_High-fidelityReversibleDataHid.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\Weng2022_Article_High-fidelityReversibleDataHid.pdf)
13. [IET Image Processing - 2022 - Zhan - Reversible data hiding for JPEG images with a cascaded structure.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\IET%20Image%20Processing%20-%202022%20-%20Zhan%20-%20Reversible%20data%20hiding%20for%20JPEG%20images%20with%20a%20cascaded%20structure.pdf)
14. [1-s2.0-S002002552101313X-main.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\1-s2.0-S002002552101313X-main.pdf)
15. [aeeev4n2spl\_10.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\aeeev4n2spl_10.pdf)
16. [Mixed-Hill-Cipher-methods-with-triple-pass-protocol-methodsInternational-Journal-of-Electrical-and-Computer-Engineering.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\Mixed-Hill-Cipher-methods-with-triple-pass-protocol-methodsInternational-Journal-of-Electrical-and-Computer-Engineering.pdf)
17. [A-new-approach-of-classical-hill-cipher-in-public-key-cryptographyInternational-Journal-of-Nonlinear-Analysis-and-Applications.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\A-new-approach-of-classical-hill-cipher-in-public-key-cryptographyInternational-Journal-of-Nonlinear-Analysis-and-Applications.pdf)
18. [1-s2.0-S1319157819304124-main.pdf](file:///C:\Users\anasu\OneDrive\Desktop\matlab\Capstone%20Project\Papers\1-s2.0-S1319157819304124-main.pdf)