Modifikasi Algoritma Controlling Expansion Dalam Meningkatan Kapasitas Penyisipan Data Hiding

Modification of the Controlling Expansion Algorithm Increasing Hiding Data Insertion Capacity

[1)], Kristoforus Fallo, [2)] Budiman Baso

[1-2)]*Program Studi Teknologi Informasi, Fakultas Sains dan Teknik, Universitas Timor*
Jl. El Tari Km.05, Kefamenanu- NTT, Indonesia 50275

Riwayat: Copyright ©2022, JITU, Submitted: 29 Agustus 2022; Revised: 1 September 2022; Accepted: 2 September 2022; Published: 30 September 2022
DOI 10.32938/jitu.v2i2.4191

Abstract – Stegonography is the art of hiding messages in other media. Stegonography is widely used to send secret messages without being known by other people by using digital media in the form of image files so that besides the sender and recipient no one knows or is aware that there is a secret message in it. Several researchers have developed these methods such as Difference Expansion, Reduced Difference Expansion, Quad Difference Expansion and Controlling Expansion. These methods have been able to recover and improve data embedding but during the running process there are several problems that often occur, namely overflow and underflow of pixel values. To overcome the above problems, we modify the Controlling Expansion algorithm by minimizing the condition of the pixel difference value and reducing the final pixel difference value after inserting the data bit and using the Location Map on the new pixel value and during secret data extraction. The experimental results show that the proposed method can increase the data storage capacity and the PSNR of stego images is higher than the previous method.

Keywords *- Stegonography; Data hiding; Controlling Expansion*

Abstrak – Stegonografi merupakan seni penyembunyian pesan kedalam media lainnya. Stegonografi banyak dimanfaatkan untuk mengirim pesan rahasia tampa diketahui oleh orang lain dengan menggunakan media digital berupa file gambar sehinga selain pengirim dan penerima tidak seorangpun ynag mengetahui atau menyadari bahwa ada suatu pesan rahasia didalamnya. Beberapa peneliti telah mengembangkan metode ini seperti Difference Expansion, Reduced Difference Expansion, Quad Difference Expansion dan Contolling Expansion metode-metode ini telah mampu memulihkan dan meningkatkan data embedding namun pada proses berjalan ada beberapa masalah yang sering terjadi yaitu overflow dan underflow nilai piksel. Untuk mengatasi masalah diatas kami memodifikasi algoritma Controlling Expansion dengan memperkecil kondisi nilai selisih piksel dan mereduksi nilai selisih piksel akhirsetelah penyisipan bit data serta menggunakan Location Map pada nilai piksel baru dan pada saat ekstraksi data secret. Hasil eksperimen menunjukan bahwa metode yang diusulkan mampu meningkatkan kapasitas penyimpanan data dan PSNR citra stego lebih tinggi dari metode sebelumnya.

Kata kunci *– stegonografi;data hiding;controlling expansion*

I. PENDAHULUAN

Perkembangan Teknologi Informasi saat in berkembang begitu pesat seiring dengan berbagai kebutuhan manusia akan informasi. Internet sebagai media akses utama manusia dalam mendapatkan berbagai sumber informasi. Hal ini akan menyebabkan tingkat penggunaan yang tinggi dan internet tidak lagi menjadi penyedia informasi yang aman karena berbagai macam masalah dalam mesin pencarian seperti spam; virus dan penyadapan.

Ada dua Teknik yang digunakan untuk meningkatkan keamanan data seperti kriptografi[1] dan stegonografi. Teknik stegonografi yaitu Teknik menyisipkan pesan data dalam media tertentu dan terlihat samar sedangkan pada kriptografi merupakan Teknik menyandingkan pesan menjadi data yang tidak dimengerti oleh orang awam. Kedua teknik memiliki perbedaan yang mendasar antara kriptografi dan stegonografi[2] yaitu citra hasial setelah dimasukan pesan rahasia didalamnya.

Pada Teknik Stegonografi ada beberapa media yang digunakan dalam menyembunyikan atau menyisipkan data seperti, media citra digital, media suara dan media video. Teknik stegonografi adalah Teknik menyembunyikan atau menyisipkan data dalam media tertentu. Tujuan dari Teknik stegonografi yaitu menyembunyikan pesan rahasia citra digital dan menghindari kecurigaan orang terhadap keberadaan pesan rahasia tersebut.

[*)] Kristoforus Fallo
Email: kristoforusfallo@unimor.ac.id

Metode yang digunakan pada Teknik stegonografi untuk menyembunyikan pesan pada citra berbeda-beda dan diklasifikasikan dalam 2 jenis yaitu *reversible*[3][4]dan *inreversible* data hiding *inreversibel* yaitu data tidak bisa dikembalikan ke daya awal dan media citra yang digunakan untuk embedin pesan tidak dapat dikembalikan kesemula atau ke citra aslinya. Metode yang sering digunakan pada kategori inreversibel[3][4]yaitu LSB (*Least Significant Bit*)[1] [5]dalam menyisipkan pesan.

Metode ini biasanya menggunakan bit-bit rendah dan menggunakan citra berskla abu-abu(*grayscale*) denga intensitas 8bit kebawah. Bit-bit data *embedded* tidak disusun berurutan pada bit-bit cover namundisusun secara acak. Keuntungan dari metode LSB adalah sederhana dan tidak dapat terlihat mata telanjang, sedangkan kelemahanya yaitu sangat sensitif terhadap penyaringan dan manipulasi stego. Pada metode Reversible gambar asli hasil stego dapat dikembalikan pada keadaan semula atau aslinya.

Ada beberapa penelitian terdahulu yang terkait *reversible* data embedding yaitu *Difference Expansion* (DE)[2][6][7],*Reduce Difference Expansion* (RDE)[8][9][10] dan *Controlling Expansion* (CE) dikembang oleh[3] mereka menggunakan 1 piksel untuk menyembunyikan 1 bit data dan kemudian dilanjutkan oleh [4] mereka menggunakan kondisi seperti dibawah ini

$$v1 = \begin{cases} \left\lfloor \frac{x+h}{2} \right\rfloor, if\ x \leq 127 \\ \left\lfloor \frac{x+h}{2} \right\rfloor, if\ x > 127 \end{cases} \quad (1)$$

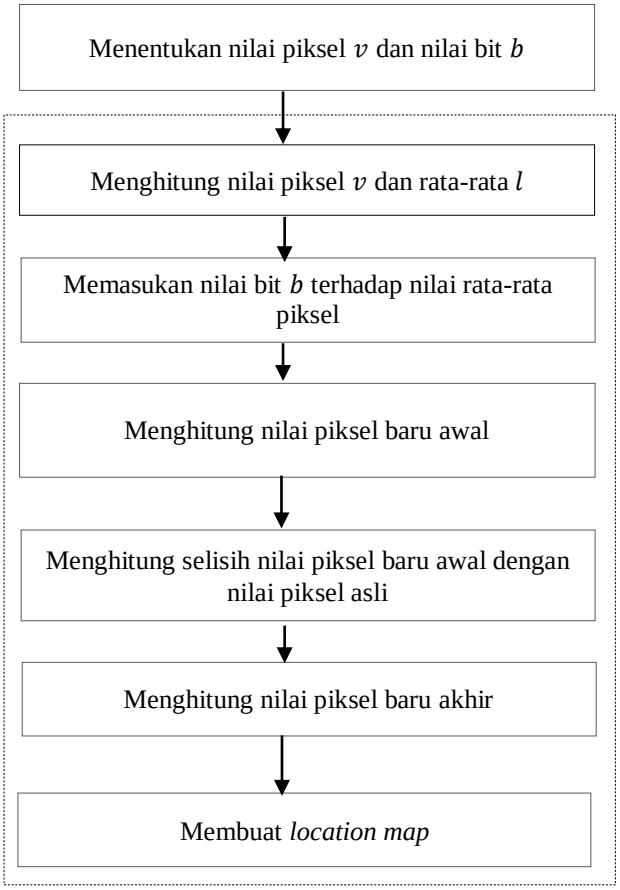
Mereka mengatakan bahwa untuk mendapatkan nilai selisih h dan nilai rata-rata dapat diperoleh dari nilai piksel itu sendiri, kondisi nilai selisih h yang sering digunakan adalah nilai 6 dan 4 tetapi permasalahan yang sering terjadi yaitu proses perhitungan selanjutnya menjadi Panjang kapasitas penyisipan menjadi berkurang. Oleh karena itu pada penelitian ini kami ingin memperbaiki metode diatas untuk mencari nilai rata-rata piksel. Dari semua penelitian diatas masih menggunakan beberapa kondisi nilai yang besar untuk memenuhi kondisi nilai rata-rata pada saat penyisipan bit data, oleh karena itu pada penelitian ini dimana mencari nilai rata-rata digunakan nilai yang kecil yaitu nilai 2 dan nilai 1.

III. METODE PENELITIAN

Metode yang diusulkan merupakan modifikasi dari metode *Controlling Expansion* sebelumnya [4]. Metode ini menggunakan satu nilai piksel untuk menyisipkan 1 bit data kedalamnya, sehinggga dari segi kapasitas metode ini sama dengan metode *Controling Expansion*. Perbedaan metode ini dengan metode sebelumnya yaitu pada kondisi untuk mencari nilai rata- rata diperkecil, dimana nilai yang diusulkan pas pada proses perhitungan selanjutnya yaitu pada saat reduksi nilai dan proses penyisipan bit data. Metode ini dapat meningkatkan kapasitas penyisipan dan mencegah *overload* [4]data yang dapat menimbulkan kecurigaan dari pembajakan data di jaringan internet.

A. Penyisipan

Penyisipan merupakan tata cara yang digunakan untuk menyimpan data didalam data cover. Data citra paling banyak digunakan sebagai cover, oleh sebab pada penelitian ini perlu dilakukan pengoperasian nilai-nilai piksel dalam citra selanjutnya yang digunakan dalam penyisipan bit data kedalamnya. Selanjutnya, tahapan pengoperasian nilai-nilai bit data dalam proses penyisipan dapat dilihat dalam gambar 1. berikut ini:



Gambar 1. Langkah-langkah penyisipan

Pada langkah pertama menentukan nilai piksel dan nilai bit [9]data, penelitian ini menggunakan citra scala abu-abu dengan intensitas 8bit dan niilai piksel beskisar 0-255. Pada nilai bit didapat dari konversi bilangan decimal ke biner menggunakan table ASCII. Tahap berikutnya adalah menghitung nilai rata-rata. Pada metode sebelumnya, untuk mendapatkan nilai selisih dan nilai rata-rata, nilai piksel ditambah beberapa nilai kondisi untuk memenuhi nilai piksel pada perhitungan selanjutnya dan juga sebagai pengurang nilai agar tidak terjadi *overflow* nilai piksel lebih setelah penyisipan bit data dan *underflow*[4] yaitu nilai piksel kurang dari nilai piksel aslinya setelah ada penambahan data rahasia. Pada metode yang diusulkan untuk menyisipkan data hanya perlu nilai 2 dan 1 untuk memenuhi kondisi nilai rata-rata

dan dapat meningkatkan kapasiatas penyisipan menggunakan persamaan (2)

$$p1 = \begin{cases} \left\lfloor \frac{v+h}{2} \right\rfloor, if\ v \leq 254 \\ \left\lfloor \frac{v+h}{2} \right\rfloor, if\ v > 254 \end{cases} \quad (2)$$

Pada persamaan (2) diatas, terdapat 2 kondisi yang harus dipenuhi oleh nilai $p1$ pada kondisi pertama jika nilai berada diantar 0-254, maka nilai piksel harus ditambah nilai 2 dan dibagi 2. Hal ini dimaksud agar tidak terjadi *overflow* (nilai piksel hasil *embedding* lebih besar dari 255) dan *underflow* (nilai piksel hasil lebih kecil dari 0). Sebagai contoh, jika nilai piksel v sama dengan 0 dan ditambah dengan 1 maka akan terjadi *underflow* jia dilanjutkan pada proses perhitungan selanjutnya, begitu juga jika nilai piksel diatas 254 dan masih ditambah 1 maka akan terjadi *overflow*. Kombinasi nilai *random* ini adalah merupakan nilai parameter terbaik untuk mendapatkan nilai $p1$ yang sesuai.

Langkah selanjutnya pada penelitian ini adalah melakukan penyisipan nilai bit b pada nilai rata-rata seperti pada persamaan (4).

$$p3 = p1 + b \quad (3)$$

Pada persamaan (4), nilai $p2$ yang telah ditambah nilai bit b kemudian nilai ini yang akan digunakan pada saat ekstraksi data atau mengembalikan nilai bit rahasia.

Pada tahap selanjutnya setelah penyisipan bit dilakukan perhitungan nilai piksel baru awal seperti pada persamaan (4).

$$v' = 2 \times p2 \quad (4)$$

Langkah selanjutnya yaitu menghitung nilai selisih piksel baru awal dengan nilai piksel asli setelah penyisipan bit data rahasia (5)

$$h' = v' - v \quad (5)$$

Langkah selanjutnya yaitu menghitung nilai piksel baru akhir (6)

$$v'' = \begin{cases} (v' - 2), if\ v' \geq 2 \\ (v' - 1), if\ v' < 2 \end{cases} \quad (6)$$

Pada persamaan (6), nilai v'' digunakan untuk menghitung nilai piksel baru akhir dari selisih nilai piksel baru awal dan nilai piksel lama setelah penyisipan bit, jika selisih nilai piksel baru awal lebih besar sama dengan 2 maka nilai piksel baru harus dikurangi 2, jika selisih nilai piksel baru awal lebih kecil 2 makan nilai piksel baru awal harus dikurangi 1, semakin kecil nilai perubahan makan semakin tinggi nilai PSNRnya.

Pada tahap selanjunya yaitu menghitung nilai *Location Map* menggunakan persamaaan (7)

$$LM = [(v'' - v)]$$

Pada persamaan (7) untuk mendapatkan nilai *Location Map* didapat dari nilai piksel asli itu sendiri. Selanjutnya ada beberapa perbaikan pada metode *controlling Expansion* yaitu dapat ditulis sebagai berikut.

$v = 255, b = 1$

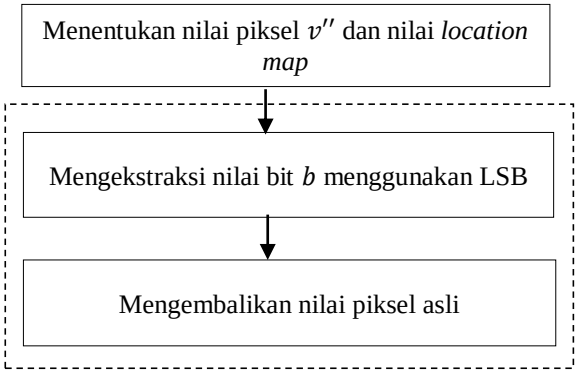
1. Menghitung nilai rata-rata
   $p1 = \lfloor (x + 2/2) \rfloor = \lfloor (255 + 2\ /2) \rfloor = 128$
2. Kemudian menghitung nilai $v3$ dan menyisipkan nilai bit b
   $p3 = (p2 + b) = (128 + 1) = 129$
3. Menghitung nilai piksel baru awal
   $v' = (2xp3) = 2x129 = 258$
4. Menghitung selisih nilai piksel baru awal dengan nilai piksel asli setelah penyisipan bit data rahasia
   $h' = (v' - v) = 258 - 255 = 3$
5. Menghitung nilai piksel baru akhir
   $v'' = (v' - 2) = (258 - 2) = 256$
6. Menhitung nilai *Location Map*
   $LM = \lfloor (v' - v) \rfloor = \lfloor (256 - 255) \rfloor = 1$

Piksel baru adalah 256 dan *location map* adalah 1. Nantinya, nilai piksel baru ini hanya bersamaan dengan nilai *location map* pada saat mengembalikan citra asli dan mengekstraksi data rahasia.

B.Proses Ekstraksi data dan Recovery image

Proses ini digunakan untuk mendapatkan data secret dan mengembalikan gambar asli dari gambar stego, pada metode-metode sebelumnya proses ini membutukan file *location map* untuk mengetahui piksel mana saja yang akan mengalami penyisipan data rahasia, serta berapa bit secret data yang disisipkan pada nilai piksel yang di proses.

Secara umum tahapan pengoperasian nilai-nilai piksel untuk mengambil nilai-nilai bit data rahasia didalam gambar stego dengan menggunakan metode yang hampir sama dengan metode yang sebelumnya, untuk mengambil data bit masih menggunakan Teknik LSB mengambil nilai bit terakhir dari masing-masing piksel, nilai LSB tersebut kemudian digabung dengan membentuk sebuah karakter yang selanjutnya dapat memberikan informasi yang diperlukan. Proses ekstraksi data dan *recoveri image* dapat disajikan pada gambar berikut 3.



Gambar 2. Langkah- langkah Ekstraksi dan recovery

Untuk proses ektraksi dan pemulihan *image*, perlu dilakukan pemilihan nilai piksel, gambar *cover* dan *Location Map* agar dapat mengembalikan nilai piksel asli.

$$b = LSB(v' + 2/2) \quad (8)$$

Dimana v' adalah nilai piksel baru setelah dimasuk data *secret*, yang kedua yaitu pulihkan gambar asli dengan nilai *stego* dengan nilai *location map* seperti pada persamaan (8), dimana nilai *location map* merupakan selisi nilai piksel asli dan nilai piksel setelah penyisipan bit data seperti pada persamaan (9).

$$v = (v' - LM) \quad (9)$$

Ini merupakan proses untuk mengembalikan nilai piksel asli, dimana kita memilih salah satu *location map* untuk mengembalikan nilai piksel asli. Untuk mengembalikan nilai piksel asli dapat digunakan cara-cara sebagai berikut: Pada proses eksraksi data menggunakan *location map* untuk proses ekstraksi.

1. Ambil nilai piksel v dan gambar yang telah disisipi bit data v'=256 dan *location map*=1
2. Menghitung nilai bit b untuk mendapat data rahasia
   $b = LSB\lfloor(v' + 2)/2\rfloor = \lfloor(256 + 2)/2\rfloor = 129$
3. Mengembalikan nilai piksel asli dengan menggunakan gambar stego dan nilai LM.
   $v = (v' - LM) = 256 - 1 = 255$

Akhirnya kita akan menemukan nilai piksel asli v adalah 255 dan bit b adalah 1.

III. HASIL DAN PEMBAHASAN

Hasil pengujian menggunakan matlab dengan akurasi metode yang diusulkan dan metode sebelumnya dalam penelitian. Beberapa nilai hasil pengujian seperti MSE dan PSNR yang digunakan untuk mengukur tingkat kualitas pada hasil penelitian tidak tetap tergantung gambar dan data secret.

Pengujian ini menggunakan gambar medis yang di ambil dari (11) dengan intensitas 8bit dengan format piksel png dan data secret menggunakan "*Lorem ipsum generator*" pada (12). Pada pengukuran dari citra stego menggunakan *Peak Signal to Noise* (PSNR)[4] yang merupakan perbandingan antar nilai maksimun dari sinyal yang diukur dalam satuan *decibel*(db). Selanjutnya PSNR digunakan untuk mengukur kualitas citra cover sebelum dan sesudah disisipkan pesan rahasia. Penentuan PSNR, terlebih dahulu harus ditentukan nilai *Mean Square Error* (MSE) yang merupakan nilai *error* kuadrat rata-rata anatara citra asli (*cover image*).

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{x=1}^{N}(S_{xy-}C_{xy})^2 \quad (10)$$

$$PSNR = 20_{log10}\frac{max|P_i|}{\sqrt{MSE}} \quad (11)$$

Berdasarkan persamaan (19) x dan y merupakan koordinat nilai piksel dari *image*, M dan N adalah dimensi atau ukuran gambar, S_{xy} menyatakan stego image dan C_{xy} cover image, untuk menghitung kapasitas menggunakan bit per pixel (cpp). Nilai cpp didapat dari membagi jumlah muatan dan jumlah piksel pada cover.

A. Pengujian

Pada pengujian metode yang diusulkan dan metode sebelumnya dengan mengukur kapasitas dan kualiatas data secret dengan melihat performance dari keduanya jika data yang disisipkan dibuat dengan ukuran piksel lokasi dan penyisipan data.

Tabel 1. Pengujian

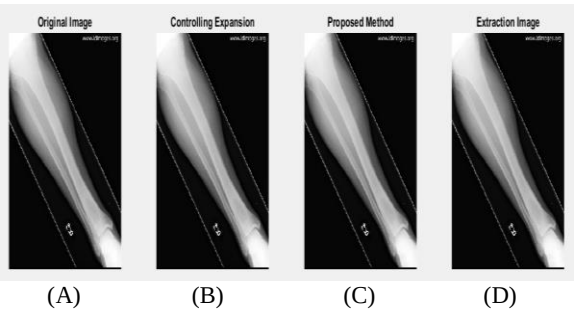
Cover image	Kapasitas (*peak signal to noise ratio*) db		
	Kapasitas(bit)	*CE*	*Proposed*
Abdominal.png	523bit	68.400	86.721
Hand.png	467bit	68.617	68.572
Lung.png	515bit	69.280	69.625
Leg.png	500bit	68.810	71.686
Rata-rata	501,25	68.776	74. 151

Berdasarkan hasil pengujian, nilai rata-rata PSNR pada data secret diukur sesuai ukuran piksel dimana piksel berukuran 523 disisipi 523bit data kedalamnya dan kualitas nilai piksel setelah disisipi pada metode CE adalah 68.400 dan untuk proposed metode yang diusulkan yaitu PSNRnya 86.725 dan juga pada piksel berukuran 500 bisa disisipi 500bit data kedalamnya dengan kualitas perbandingan pada metode CE PSNR 68.810 dan metode yang diusulkan 71.686.

Pada pengujian ini juga dihitung nilai rata-rata PSNR kedua metode, pada metode CE rata-rata PSNR 68.774 dan pada metode yang diusulkan jauh diatas metode CE yaitu rata-rata PSNR 74.151. pengujian kedua metode ini dibatasi oleh jumlah piksel dan data secret.

IV. KESIMPULAN

Penelitian ini menyajikan sebuah metode yang mampu meningkatkan kapasiatas penyisipan data secret dengan mengggunakan 1 nilai *pixel* dan dari segi keamanan menggunakan *location map* pada piksel baru dan pada saat ekstraksi data. Pada penelitian selanjut kami ingin memperluas lagi bit data penyisipan.



(A) (B) (C) (D)

(E) (F) G) (H)

Gambar 3. (A) Leg.png, (B)Leg.png CE, (C) Leg.png Proposed, (D) Leg.png Recovery, (E) Hand.png, (F) Hand.png CE,), (H) Hand.png Proposed, (G) Hand.png Recovery

DAFTAR PUSTAKA

[1] M. F. Syawal, D. C. Fikriansyah, and N. Agani, "Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB," vol. 4, no. 3, 2016.

[2] T. Ahmad, "Increasing the Performance of Difference Expansion-based Steganography when Securing Medical Data," no. December, 2015, doi: 10.6029/smartcr.2014.04.007.

[3] D. S. Angreni and T. Ahmad, "Enhancing DE-based Data Hiding Method by Controlling the Expansion".

[4] T. Ahmad and S. S. Manek, "Securing secret data by enhancing the controlling expansion method," *ICIC Express Letters, Part B: Applications*, vol. 9, no. 11, pp. 1091–1099, 2018, doi: 10.24507/icicelb.09.11.1091.

[5] H. Antonio, "DENGAN MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DAN END OF FILE".

[6] J. Tian, "Reversible Data Embedding Using a Difference Expansion," vol. 13, no. 8, pp. 890–896, 2003.

[7] P. Maniriho, L. Jovial, Z. Bizimana, and E. Niyigaba, "Reversible difference expansion multi-layer data hiding technique for medical images," vol. 7, no. 1, pp. 1–11, 2021.

[8] T. Informatika and F. T. Informasi, "PENGGUNAAN KLASTER PIKSEL UNTUK MENINGKATKAN KINERJA REDUCED DIFFERENCE EXPANSION," vol. 4, no. 3, pp. 135–140, 2015.

[9] L. Amalia, T. Ahmad, L. Amalia, and T. Ahmad, "Jurnal Rekayasa Elektrika dan Reduced Difference Expansion," vol. 13, no. 36, 2017, doi: 0.17529/jre.v13i2.7612.

[10] Z. Syahlan and T. Ahmad, "Reversible data hiding method by extending reduced difference expansion," vol. 5, no. 2, pp. 101–112, 2019.

[11] Partners Infectious Disease Images - eMicrobes Digital Library - Home." [Online]. Available: http://www.idimages.org/. [Accessed: 10- Dec-2016].

[12] Lorem Ipsum - All the facts - Lipsum generator." [Online]. Available: http://www.lipsum.com/. [Accessed: 10-Dec-2016].